EU:n tietosuojalainsäädännön vaikutus kolmansissa maissa

OTM-tutkielma
Helsingin yliopisto
Oikeustieteellinen tiedekunta
Oikeusteoria
Joulukuu 2018
Tekijä: Anna-Eliina Simola
Ohjaajat: Panu Minkkinen ja
Heikki Pihlajamäki

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Tiedekunta/Osasto Fakultet/Sektion – Faculty Oikeustieteellinen tiedekunta	Laitos/Institution– Department	
Tekijä/Författare – Author Anna-Eliina Simola		
Työn nimi / Arbetets titel – Title EU:n tietosuojalainsäädännön vaikutus kolmansissa maissa		
Oppiaine /Läroämne – Subject Oikeusteoria		
Työn laji/Arbetets art – Level OTM-tutkielma	Aika/Datum – Month and year 12/2018	Sivumäärä/ Sidoantal – Number of pages IV + 94

Tiivistelmä/Referat – Abstract

Tässä tutkielmassa tarkastellaan EU:n tietosuojalainsäädännön vaikutusta EU:n rajojen ulkopuolella kolmansissa maissa. Henkilötietojen suojan merkitys on viime aikoina noussut huomattavasti teknologian kehityksen ja internetin seurauksena. EU:ssa henkilötietojen suojalla ja yksityisyydellä on vahva perusoikeusasema, ja hiljattain sovellettavaksi tullut tietosuoja-asetus parantaa henkilötietojen suojaa EU:ssa entisestään. Internetin globaalin luonteen takia ei kuitenkaan riitä, että henkilötiedot on suojattu vain EU:n alueella. Samoin henkilötiedoilla on suuri merkitys taloudellisessa toiminnassa, minkä takia henkilötietoja siirretään ympäri maailmaa. Toteuttaakseen tavoitteensa kattavasta henkilötietojen suojasta EU:n tulisi siten pystyä vaikuttamaan rajojensa ulkopuolellakin.

EU voi pyrkiä vaikuttamaan perinteisesti kansainvälisten ihmisoikeussopimusten ja -julistusten kautta tai ottamalla henkilötietojen suojan esille kolmansien maiden kanssa käytävissä neuvotteluissa. Vaikuttaminen tätä kautta on kuitenkin vaikeaa ja saattaa törmätä kolmansien maiden suvereeniuteen. Kolmansissa maissa voi olla henkilötietojen suojasta ja yksityisyydestä hyvin erilaisia näkemyksiä kuin EU:ssa, jolloin myöskään esimerkiksi EU:n tietosuojalainsäädäntöä vastaavia normeja ei haluta.

Hienovaraisemmin EU voi vaikuttaa markkinatalouden ja yritysten toiminnan kautta. EU on tarpeeksi suuri markkinavoimaltaan ja tehokas toiminnaltaan, jolloin ns. Bryssel-efektin on mahdollista toteutua. Tällöin EU:n säännellessä omia sisämarkkinoitaan sen lainsäädäntöä tosiasiasiallisesti noudatetaan taloudellisista syistä myös kolmansissa maissa. Kolmas ja pehmein vaihtoehto vaikuttaa on ohjata ihmisten käyttäytymistä. Ihmisten asenteita voidaan yrittää muuttaa, jolloin EU:n ajatusmalli henkilötietojen suojasta leviäisi muualle. Ihmisten käyttäytymistä muuttamalla voidaan vaikuttaa myös yritysten toimintaan, jolloin niiden muuttaessa toimintaansa voidaan mahdollisesti vaikuttaa ihmisten käyttäytymiseen laajemmin.

Tutkimuksessa keskitytään nimenomaan lainsäädännön tosiasiallisesti ilmenevään vaikutukseen. EU:n tietosuojalainsäädännön mahdollista ekstraterritoriaalista vaikutusta tutkitaan tarkemmin oikeuden tulla unohdetuksi ja rajatylittävien henkilötietojen siirtojen kautta. Näiden yhteydessä esille nousevat EUT:n ratkaisuista etenkin tapaukset C-131/12 Google Spain ja C-362/14 Schrems. Tapausten perusteella voidaan havaita, että EU:lla on valtaa vaikuttaa rajojensa ulkopuolella mutta kaikissa tilanteissa se ei kuitenkaan onnistu.

Avainsanat – Nyckelord – Keywords
henkilötiedot, yksityisyys, EU, tietosuoja-asetus, ekstraterritoriaalisuus, perus- ja ihmisoikeudet, Bryssel-efekti

Säilytyspaikka – Förvaringställe – Where deposited

Muita tietoja – Övriga uppgifter – Additional information

Sisällysluettelo

Lyhenteet

AEPD	Agencia Española de Protección de Datos
ASEAN	Association of Southeast Asian Nations
CNIL	Commission nationale de l'informatique et des libertés
EIS	Euroopan ihmisoikeussopimus
EIT	Euroopan ihmisoikeustuomioistuin
EU	Euroopan unioni
EUT	Euroopan unionin tuomioistuin
GATS	General Agreement on Trade in Services
HTD	Henkilötietodirektiivi: Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta
Ihmisoikeusjulistus	Yhdistyneiden Kansakuntien yleismaailmallinen ihmisoikeuksien julistus
KP-sopimus	Yhdistyneiden Kansakuntien kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus
NSA	National Security Agency
PL	Perustuslaki (731/1999)
POK	Euroopan unionin perusoikeuskirja
SEU	Sopimus Euroopan unionista
SEUT	Sopimus Euroopan unionin toiminnasta
TSA	Tietosuoja-asetus: Euroopan parlamentin ja neuvoston asetus 2016/679/EU luonnollisten henkilöiden suojelusta henkilötieto-

	jen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta
WTO	World Trade Organization, Maailman kauppajärjestö
YK	Yhdistyneet Kansakunnat

1. Johdanto

1.1. Taustaa ja tutkimuskysymys

”Ei ole mitään kätkettyä, mikä ei tulisi ilmi, eikä salattua, mikä ei paljastuisi ja tulisi tietoon.” (Luuk. 8:17)

Yhteiskunta on muuttunut lähihistorian aikana luultavasti nopeammin kuin koskaan aiemmin koko ihmishistoriassa. Teknologian, internetin ja digitalisaation myötä nykyihmisen elämä näyttää täysin erilaiselta kuin vasta sata vuotta sitten. Nykyisin suuri osa elämästämme on tiiviisti yhteydessä teknologiaan ja riippuvaista siitä. Älypuhelimemme tuntevat meidät luultavasti paremmin kuin me itse, ja selaimen selaushistoriasta voi saada hyvinkin kattavan kuvan ihmisen persoonasta ja elämästä. Henkilötiedoista on tullut uutta valuuttaa, ja niiden avulla esimerkiksi tehdään kohdennettua mainontaa ja tarjotaan yksilöllisesti räätälöityjä palveluja. Henkilötiedot toimivat usean yrityksen toiminnan raaka-aineena. Samalla kun teknologia on helpottanut elämäämme, sen mukana on syntynyt uusia uhkia yksityisyydelle ja henkilötietojen suojalle, sillä tietojen kerääminen ja laajamittainen analysointi on nykyisin sekä mahdollista että hyvin vaivatonta. Puhelimet, tietokoneet, tabletit ja älykellot keräävät henkilötietoja ilman, että ihmiset itse edes ymmärtävät sitä. Henkilötietojen suoja on välttämätöntä, jotta esimerkiksi oikeus yksityisyyteen säilyy ja jotta yksilö olisi suojassa perusteettomalta vakoilulta ja tarkkailulta.

Tämän tutkimuksen aiheena on, kuinka EU:n tietosuojasääntely vaikuttaa EU:n alueen ulkopuolella eli ekstraterritoriaalisesti kolmansissa maissa. EU:ssa on jo 1990-luvulla säännelty henkilötietojen suojasta henkilötietodirektiivillä (95/46/EY, myöhemmin myös HTD). Muutosten myötä tarvitaan kuitenkin aiempaa tiukempaa lainsäädäntöä, jotta estettäisiin henkilötietojen suojaan ja yksityisyyteen kohdistuvia uhkia sekä taattaisiin rekisteröidylle eli henkilötietojen kohteelle vahvemmat oikeudet. Tähän tarpeeseen säädettiin tietosuoja-asetus (2016/679/EU, myöhemmin myös TSA). Vuonna 2012 EU:n silloinen oikeuskomissaari Viviane Reding lausui: ”Euroopan tietosuojalainsäädännöstä tulee tavaramerkki, jonka ihmiset tunnustavat ja johon he luottavat maailmanlaajuisesti.” [1] Tavoitteena oli siten luoda globaalilla tasolla merkityksellistä lainsäädäntöä. Koska internet ei tunne rajoja, ja suuret teknologiajätit ovat niin ikään luonteeltaan globaaleja, henkilötieto-

[1] http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm “European data protection rules will become a trademark people recognise and trust worldwide.” (Käännös tässä)

jen suojasta säänteleminen on haastavaa, sillä suojan kattava toteutuminen vaatii, että tiedot on suojattu kaikkialla, missä niitä käsitellään ja säilytetään. Mikäli muualla henkilötiedoille ei ole taattu suojaa, EU:n tulee ulottaa sen tietosuojasääntely oikeudenkäyttöpiirinsä ulkopuolelle omalla alueellaan olevien ihmisten henkilötietojen suojan turvaamiseksi. Se, kuinka tämä tapahtuu vai tapahtuuko sitä, on tutkimuksen kohteena.

Miksi henkilötiedoilla sitten loppujen lopuksi on niin suuri merkitys? Tieto on valtaa, ja niiden avulla saadaan rahaa. Rahalla puolestaan voidaan hankkia lisää tietoa ja valtaa, ja näin itseään ruokkiva kehä on valmis. Ne, joilla on tietoa muista ihmisistä, voivat ensinnäkin vaikuttaa heihin helpommin — jopa ilman, että kohde edes sitä itse ymmärtää. Toisekseen tieto myös mahdollistaa ihmisten kontrolloimisen tehokkaasti. Henkilötiedoissa on kyse siten paljon muustakin kuin vain yksilön mahdollisuudesta päättää, minkälaisena ihmisenä hänet yksityisyyden piirinsä ulkopuolella nähdään, vaikka myös tämä on yksilölle itselleen merkityksellistä. Henkilötietojen suoja yhdessä yksityisyyden kanssa merkitsee, ettei muilla, kuten valtiolla tai suuryrityksellä, ole niin suurta vaikutusvaltaa yksilöön. Tämä onkin mahdollisesti suurempi syy vastustaa parempaa tietosuojaa kuin mahdolliset kulttuuriset erot siitä, mitä pidetään yksityisenä ja kuinka tärkeänä henkilötietojen suojaa pidetään. Sen takia on myös merkityksellistä, kenen sääntelyä henkilötietojen suojasta ja käsittelystä noudatetaan.

Yleisenä rajauksena ja lähtökohtana tutkielmassa on, että kohteena on vain toiminta, joka kuuluu EU:n lainsäädännön soveltamisalaan. Muutoinhan EU:n sääntely ei tule sovellettavaksi. Lisäksi lähtökohtaisesti rekisterinpitäjänä pidetään yritystä, vaikka monet muutkin tahot voivat olla rekisterinpitäjiä. Selvyyden vuoksi myös puhutaan vain rekisterinpitäjistä kiinnittämättä sen enempää huomiota henkilötietojen käsittelijöihin eli tahoihin, jotka käsittelevät henkilötietoja rekisterinpitäjän lukuun.

1.2. Tutkimuksen menetelmä

Oikeustieteessä menetelmällä tarkoitetaan pikemminkin valittua näkökulmaa oikeuteen kuin yksiselitteistä kaavaa, jota soveltamalla löydettäisiin vastaus.[2] Yksityisyyden ja henkilötietojen suojan käsitteet sekä näiden välinen suhde on tarpeen määritellä aluksi, jotta lukijalla olisi käsitys niiden sisällöstä ja perusteista myöhempää varten. Tässä apuna käytetään eri teorioita. Tutkimuksen lähestymistapa on alussa siten oikeusteoreettinen, mikä

[2] Aarnio 1997, s. 35–36.

tarkoittaa oikeuden yleisten kysymysten tutkimista ja joka antaa kokonaiskuvan oikeudesta ja sen käsitteistä.[3]

Perinteisessä oikeusdogmaattisessa eli lainopillisessa tutkimuksessa oikeutta pidetään itsenäisenä, ja keskeistä on selvittää voimassa olevan lain sisältö.[4] Lainopilla voimassa olevia normeja systematisoidaan ja tulkitaan ja tätä kautta saadaan myös selville todellisuus normien maailmassa.[5] Tässä tutkimuksessa tarkastellaan kuitenkin EU:n lainsäädännön tosiasiallista vaikutusta kolmansissa maissa, joten oikeutta ei voida käsitellä erillisenä entiteettinä, eikä vastausta voida löytää pelkästään normeja tulkitsemalla. Lähtökohtana tutkimuksessa on, että yhteiskunta, kulttuuri ja oikeus ovat toisiinsa kietoutuneita. Oikeus ei ole ympäröivästä maailmasta ja sen vaikutuksista erillinen, autonominen alueensa, vaan se on vuorovaikutuksessa sitä ympäröivän yhteiskunnan ja kulttuurin kanssa. Oikeutta lähestytään tutkimuksessa siten oikeus ja yhteiskunta -näkökulmasta, jossa oikeudellisia ilmiöitä tarkastellaan konkreettisesta maailmasta käsin.[6] Oikeus ja yhteiskunta -näkökulmassa lakia ja oikeutta voidaan lähestyä hyvin laajasti eri lähtökohdista, joten tarkemmin sanottuna tutkimuksen menetelmä on kontekstuaalinen laintutkimus.[7]

Ennen kuin EU:n tietosuojalainsäädännön vaikutusta voidaan tarkemmin tutkia, täytyy normeja ensin systematisoida, jotta niiden sisältö ymmärretään. Tässä apuna käytetään muun muassa EUT:n ratkaisuja ja komission tiedonantoja. Lainopillisella menetelmällä lähtökohtaisesti etsitään vastausta yksittäiseen oikeudelliseen kysymykseen. Tässä tutkimuksessa kuitenkin arvioidaan lainsäädännön tosiasiallisia vaikutuksia kansainvälisesti, joten vaikka tutkimuksessa tehtävä oikeuden systematisointi on samankaltaista lainopin kanssa, käytetty oikeus ja yhteiskunta -menetelmä vetää tutkimusta systematisoinnin jälkeen lainopista poikkeavaan suuntaan. Tutkimuksessa konteksti huomioidaan siten, että yksityisyyden ja henkilötietojen suojan ihmisoikeusasemaa eri puolilla maailmaa tarkasteltaessa huomioidaan lain kirjaimen lisäksi myös ympäröivä kulttuuri. Samoin EU:n tietosuojalainsäädännön kolmansissa maissa tapahtuvan *de facto* vaikutuksen arvioinnissa otetaan huomioon markkinatalous ja sen toiminta, eikä niinkään keskitytä kolmansien maiden tietosuojalainsäädäntöön. Vaikutuksen syntymisen arvioinnissa apuna käytetään etenkin Bryssel-efektiä.

[3] Hirvonen 2011, s. 27.
[4] Twining 1997, s. 39.
[5] Hirvonen 2011, s. 22.
[6] Twining 2009, s. 226.
[7] ”Law in context”. Menetelmällä ei ole suomessa varsinaisesti vakiintunutta termiä.

1.3. Tutkimuksen rakenne

Tutkielman rakenne etenee yleisemmästä käsittelystä erityisempään. Aluksi luodaan pohjaa henkilötietojen suojasta ja yksityisyydestä, minkä jälkeen siirrytään varsinaisesti tutkimuskysymyksen pariin. Toisessa luvussa käydään lyhyesti läpi, mistä yksityisyydessä ja henkilötiedoissa on kyse ja haetaan niille mahdollisia määritelmiä. Tutkimus keskittyy henkilötietojen suojaan, mutta oikeus yksityisyyteen on sen kannalta tärkeä. Tämän takia toisen luvun lopussa pohditaan yksityisyyden ja henkilötietojen suojan välistä suhdetta. Jotta lukija saa käsityksen kyseisten oikeuksien asemasta ja merkityksestä EU:n ulkopuolella, kolmannessa luvussa tarkastellaan oikeuden yksityisyyteen ja henkilötietojen suojan universaaliutta. Samalla tutkitaan kyseisten oikeuksien mahdollisia törmäyksiä muiden perus- ja ihmisoikeuksien, lähinnä sananvapauden kanssa. Oikeuksien välisessä punninnassa on eroja eri maiden välillä, mikä voi aiheuttaa ristiriitaa EU:n normien tunkeutuessa alueensa ulkopuolelle.

Kun on muodostettu käsitys sekä henkilötiedoista, yksityisyydestä että niiden maailmanlaajuisesta asemasta, siirrytään tutkimaan EU:n valtaa, EU:n tietosuojanormien sisältöä ja niiden vaikutusta EU:n ulkopuolella kolmansissa maissa. Neljännessä luvussa tutkitaan EU:n vaikutusvaltaa ja keinoja sen käyttämiseen kansainvälisessä kentässä. Tavat vaikuttaa on jaettu kolmeen osaan eli vaikuttamiseen kansainvälisillä sopimuksilla tai neuvotteluilla, vaikuttamiseen markkinataloutta hyväksikäyttämällä Bryssel-efektin avulla ja vaikuttamiseen käyttäytymistä ohjaamalla.

Tämän jälkeen EU:n tietosuojanormien vaikutusta tarkastellaan kahden esimerkin kautta. Viidennessä luvussa keskitytään oikeuteen tulla unohdetuksi, joka on yksi EU:n tietosuojalainsäädännössä rekisteröidylle taatuista oikeuksista. Tarkastelun keskiössä on EUT:n Google Spain -tapaus (C-131/12), jonka avulla selvitetään, mistä oikeudessa on ensinnäkin kyse ja sen mahdollisesta ulottumisesta kolmansiin maihin. Kuudennessa luvussa EU:n tietosuojalainsäädännön ekstraterritoriaalista vaikutusta tutkitaan henkilötietojen rajatylittävien siirtojen kautta. Henkilötietojen siirrossa mukaan tulee vahvasti henkilötietojen liityntä talouteen, joka tuo EU:n tietosuojasääntelyn vaikutukselle uusia ulottuvuuksia. Tästä liitynnästä huolimatta myös perusoikeus näkökulma on henkilötietojen siirrossa vahva, kuten kuudennessa luvussa käsiteltävästä EUT:n Schrems-tapauksesta (C-362/14) ilmenee. Tämän jälkeen on loppupäätelmien vuoro.

2. Yksityisyys ja henkilötietojen suoja

Tässä luvussa käydään ensin läpi normiperustaa oikeudelle yksityisyyteen sekä henkilötietojen suojalle niin kansainvälisesti kuin EU:ssa ja kansallisella tasolla. Tämän jälkeen käsitellään eri yksityisyyttä selittäviä teorioita, joista ilmenee, ettei yksiselitteistä määritelmää yksityisyydelle ole. Tämä on tarpeen, jotta lukija ymmärtäisi myöhemmin kolmannessa luvussa esille tulevan ongelman siitä, kuinka monimuotoisesti yksityisyys voidaan käsittää. Yksityisyyden lisäksi määritellään henkilötietojen suojaa sekä sitä, kuinka henkilötietoja voidaan hahmottaa yksityisyyttä käsittelevät teorioilla. Henkilötietojen suojaa pidetäänkin usein yksityisyyden alakategoriana. Nähdäkseni tämä näkökulma on kuitenkin puutteellinen, sillä henkilötietojen suojalla on myös itsenäisiä intressejä. Tämän takia luvun lopussa käsitellään näiden oikeuksien välistä suhdetta, koska myöhemmin tutkimuksessa henkilötietojen suojasta puhutaan lähtökohtaisesti rinnakkaisena oikeutena yksityisyyden kanssa eikä sille alisteisena.

2.1. Oikeuden yksityisyyteen ja henkilötietojen suojan normiperusta

2.1.1. Kansainvälinen normiperusta Euroopasta tarkasteltuna

Vaikka oikeus yksityisyyteen on suhteellisen uusi ajatus, se on silti erittäin laajalti hyväksytty moraalisena oikeutena.[8] Se ei ole kuitenkaan jäänyt vain moraalisen oikeuden tasolle, vaan sillä on vahva normiperusta. Ehdottomasti tunnetuin kansainvälinen julistus on YK:n yleismaailmallinen ihmisoikeuksien julistus (ihmisoikeusjulistus), jonka 12 artiklan mukaan

> *”Älköön mielivaltaisesti puututtako kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon älköönkä loukattako kenenkään kunniaa ja mainetta. Jokaisella on oikeus lain suojaan sellaista puuttumista tai loukkausta vastaan.”*

Ihmisoikeusjulistuksen jälkeen YK:ssa laaditun kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen (KP-sopimus) 17 artiklassa turvataan samoin oikeus yksityisyyteen. Kuten ihmisoikeusjulistuskin, artikla kieltää mielivaltaisen tai laittoman puuttumisen yksilön yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon sekä suojaa yksilöä kunnian ja maineen loukkauksilta.

[8] Rickless 2007, s. 773, ja Himma 2007 s. 856, 859.

Euroopasta katsottuna kansainvälisellä tasolla erittäin tärkeässä asemassa on Euroopan neuvoston Euroopan ihmisoikeussopimus (EIS). Oikeus yksityisyyteen on turvattu sen 8 artiklassa, jonka mukaan

> *”1. Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta.”*

EIS:n tarjoama suoja on yksilölle konkreettista, sillä hän voi viedä kokemansa oikeudenloukkauksen EIT:lle harkittavaksi. Sen sijaan YK:n kohdalla ongelmana on, että suoja jää tosiasiallisesti epämääräiseksi, vaikka kansainväliset sopimukset periaatteessa sitovatkin sopimuksien osapuolina olevia valtiota. YK:lta nimittäin puuttuu tehokas oikeuksien täytäntöönpanomekanismi, joten valtion rikkoessa sopimusta ei siitä useinkaan aiheudu valtiolle muita varsinaisia seurauksia kuin mahdollisesti kansainvälistä poliittista painostusta. Siten vaikka oikeus yksityisyyteen on turvattu YK:n KP-sopimuksessa, ei yksittäinen ihminen saa siitä paljoakaan suojaa itselleen, mikäli valtio ei jostain syystä halua noudattaa sitä itseään sitovaa sopimusta.

Edellä mainituissa sopimuksissa selkeästi suojataan oikeus yksityisyyteen, mutta henkilötietojen suojasta niissä ei puhuta mitään. Henkilötietojen suojan käsitetäänkin kuuluvan yksityisyyden alle ja kyseisten artiklojen katsotaan antavan suojaa henkilötiedoille nimenomaisen ilmaisun puutteesta huolimatta.[9] Ihmisoikeusjulistuksen, KP-sopimuksen ja EIS:n lisäksi on olemassa monia muitakin kansainvälisiä ihmisoikeussopimuksia ja -julistuksia, joista puhutaan tarkemmin luvussa kolme, jossa tarkastelu siirtyy Euroopan ulkopuolelle.

2.1.2. EU:n sääntely yksityisyydestä ja henkilötietojen suojasta

EU:n perusoikeuskirjan (POK) 7 artiklassa on yksityisyyden suojasta hyvin samanlainen linjaus kuin EIS:ssa. Kyseisen artiklan mukaan

> *”Jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan*.”

Ulkonaisesti POK 7 artikla ei oikeastaan poikkea siitä, mitä EIS:ssa yksityisyydestä on säädetty. Sen sijaan paneuduttaessa tarkemmin henkilötietojen suojaan on havaittavissa selkeä ero. POK:ssa on nimittäin erikseen säädetty henkilötietojen suojasta sen 8 artiklassa,

[9]Lynskey 2014, s. 569–570.

joten henkilötiedot eivät kuulukaan oikeuden yksityisyyteen alle kuten EIS:ssa. POK 8 artiklan mukaan

> *”1. Jokaisella on oikeus henkilötietojensa suojaan.*
>
> *2. Tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi.”*

Lisäksi SEUT 16(1) artiklan mukaan ”jokaisella on oikeus henkilötietojensa suojaan.” Vaikuttaakin siltä, että EU:ssa henkilötietojen suoja on otettu vakavasti, koska se on erikseen kirjattu sekä perusoikeuskirjaan että perustamissopimukseen. Koska POK on laadittu EIS:a ja KP-sopimusta huomattavasti myöhemmin, henkilötietojen suojan merkityksen kasvu on siinä voitu huomioida paremmin vastaamaan nykyisen yhteiskunnan tarpeita ja osoittaa henkilötietojen suojalle omaa painoarvoa. Suurten tietomassojen käsittelyn ja analysoinnin tultua mahdolliseksi henkilötietojen monipuolisempi hyväksikäyttö ja samalla ihmisten yksityisyyteen tunkeutuminen on tullut aiempaa helpommaksi. Näin ollen henkilötietojen suojan tarve on kasvanut huomattavasti viime aikoina.

Asetus- ja direktiivitasolla on mahdotonta säännellä yleisesti yksityisyydestä sen moniulotteisuuden ja abstraktin luonteen takia. Yksityisyydestä sääntely toteutuu siten aina jonkun siihen kuuluvan osa-alueen kautta, esimerkiksi viestintää koskevassa sääntelyssä. Henkilötietojen suoja on sen sijaan konkreettisempaa. Niinpä henkilötietojen suojalle on EU:ssa omistettu oma asetuksensa, tietosuoja-asetus, joka luo pohjan henkilötietojen käsittelylle ja suojalle EU:ssa ja on EU:n tärkein henkilötietoihin liittyvä normisto. Samalla tietosuoja-asetus myös osittain sääntelee oikeudesta yksityisyyteen, koska tarkoituksena on henkilötietojen suojan kautta suojata ihmisten yksityisyyttä.[10] EU:ssa on lisäksi useita muita direktiivejä ja asetuksia, joilla säännellään niin henkilötiedoista kuin yksityisyydestäkin. Tällaisia ovat esimerkiksi viranomaisten tietojenkäsittelydirektiivi (2016/680/EU) tai sähköisen viestinnän tietosuojadirektiivi (58/2002/EY)[11].

[10] TSA johdanto, kohta 4.
[11] Tämä direktiivi tullaan lähitulevaisuudessa korvaamaan sähköisen viestinnän tietosuoja-asetuksella, ks. COM (2017) 10.

EU:n asetukset ovat jäsenvaltioissa suoraan sovellettavaa oikeutta. SEUT 288 artiklan toisen kappaleen mukaan: ”Asetus pätee yleisesti. Se on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.” Siten tietosuoja-asetus vaikuttaa kaikissa EU:n jäsenvaltioissa ilman implementointia ja sillä on välitön oikeusvaikutus. EU-oikeuden etusijaperiaate mahdollistaa suoran sovellettavuuden ja välittömän oikeusvaikutuksen tosiasiallisen toteutumisen.[12] Jos jäsenvaltiolla on asetuksesta poikkeavaa kansallista sääntelyä, asetus syrjäyttää sen etusijaperiaatteen mukaisesti, kun kyse on EU:n toimivaltaan kuuluvasta asiasta.

Ennen yleistä tietosuoja-asetusta henkilötietojen suojasta EU:ssa säänneltiin henkilötietodirektiivillä, jonka kukin jäsenvaltio oli implementoinut omaan kansalliseen lainsäädäntöönsä. Tästä syntyi väistämättä eroja jäsenvaltioiden välille, joten tietosuoja-asetuksen voimaantulo muutti tilannetta huomattavasti antaen kaikille täysin samat normit. Suoran sovellettavuuden ja välittömän oikeusvaikutuksen seurauksena tietosuoja-asetuksesta käytännössä tulee osa kansallista oikeutta, vaikka kansallinen lainsäätäjä ei olekaan sitä säätänyt.

2.1.3. Kansallinen normiperusta

Suomessa sekä oikeus yksityisyyteen että henkilötietojen suoja on huomioitu perustuslain (PL, 731/1999) tasolla. PL 10 §:n mukaan

> *”Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla.*
>
> *Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.”*

Kyseistä pykälää täydentävät muun muassa yleislakina henkilötietolaki (523/1999) sekä laki yksityisyyden suojasta työelämässä (759/2004). Yksityisyyttä ja henkilötietojen suojaa koskevia säännöksiä on myös laissa viranomaisten toiminnan julkisuudesta (ns. julkisuuslaki 621/1999) sekä laissa sähköisen viestinnän palveluista (ns. tietoyhteiskuntakaari, 917/2014). Lisäksi näiden oikeuksien rajoittamisesta on säädetty esimerkiksi pakkokeinolaissa (806/2011), jossa mahdollistetaan muun muassa televalvonta ja -kuuntelu tietyissä tilanteissa. Jo näin lyhyt listaus osoittaa, kuinka monessa eri yhteydessä yksityisyys ja henkilötietojen suoja nousevat esille.

[12] Suorasta sovellettavuudesta, välittömästä oikeusvaikutuksesta ja EU-oikeuden etusijasta ks. EUT:n ratkaisut C-26/62 (Van Gend en Loos), C-6/64 (Costa v. ENEL) ja C-106/77 (Simmenthal).

Henkilötietolaki perustui entiseen henkilötietodirektiiviin ja kyseinen laki tullaankin kumoamaan uudella, EU:n tietosuoja-asetuksen kanssa sopusoinnussa olevalla tietosuojalailla. Jo nyt tietosuoja-asetus syrjäyttää henkilötietolain säännökset edellisessä kappaleessa esitetyn mukaisesti, jos ne ovat tietosuoja-asetuksen kanssa ristiriidassa. Luonnollisesti näin käy myös uuden tietosuojalain kohdalla, jos jokin sen pykälistä ei olisikaan tietosuoja-asetuksen mukainen. Ainoastaan tilanteissa, jotka eivät kuulu EU:n toimivallan piiriin, voidaan noudattaa tietosuoja-asetuksesta poikkeavia kansallisia normeja. Tulevan tietosuojalain tarkoituksena on täydentää tietosuoja-asetusta ja soveltaa sitä tietosuojalain rinnalla eikä olla itsenäinen sääntelykokonaisuutensa,[13] joten ristiriitoja pyritään välttämään.

Vaikka EU on henkilötietojen suojassa ottanut lainsäädännöllisesti järeämmän keinon käyttöön eli säätänyt henkilötiedoista direktiivin sijaan asetuksella, tietosuoja-asetuksessa on annettu jäsenvaltiolle myös liikkumavaraa. Tietosuoja-asetuksessa jäsenvaltioille on annettu harkintamarginaalia esimerkiksi 23 artiklassa koskien rekisteröityjen oikeuksien rajoittamista kansallisella lailla tai 85 artiklassa koskien sanan- ja tiedonvälityksen vapauden yhteensovittamista henkilötietojen suojan kanssa. Joissain kohdin annettu liikkumavara on mahdollisuus, mutta osa artikloista asettaa tarkemman sääntelyn jäsenvaltion velvollisuudeksi, kuten on esimerkiksi edellä mainitun TSA 85 artiklan kohdalla.[14] Tämän avulla jäsenmaiden on tietyssä mittakaavassa mahdollista ottaa huomioon oman yhteiskuntansa erityispiirteitä, mutta henkilötietojen suojasta säädettyä kovaa ydintä ja tietosuoja-asetuksen kokonaiskuvaa ei ole mahdollista muuttaa. Liikkumavarassa onkin kyse vain pienestä lainsäädännöllisestä hiomisesta.

2.2. Määritelmiä ja teoriaa

Monista normeista huolimatta oikeus yksityisyyteen on erittäin epäselvä konsepti, ja oikeuskirjallisuudessa on todettu, ettei oikein kukaan tiedä, mitä se varsinaisesti on.[15]. Koska yksityisyyden ja sen piirin määritteleminen on niin subjektiivista, ei yhteistä ja selkeää määritelmää ole löydettävissä. Myöskään EIT ei ole oikeuskäytännössään edes pyrkinyt määrittelemään yksityisyyttä, vaan on katsonut sen mahdottomaksi.[16] Epämääräisyydestä johtuen yksityisyydelle on pyritty luomaan monia eri teorioita. Teoriat ovat yhtä mieltä siitä, että oikeudessa yksityisyyteen suoja tulee henkilökohtaisille ja intiimeille asioille, ei

[13] HE 9/2018 vp, s. 1.
[14] Ks. liikkumavarataulukko OMML 35/2017, s. 48–67.
[15] Thomson 1975, s. 295, Rickless 2007, s. 773, ja Solove 2009, s. 1–2.
[16] Niemietz vs. Saksa, kohta 29.

julkiseen piiriin kuuluville tiedoille.[17] Tämä on itsestään selvää, mutta siihen yhtäläisyydet loppuvatkin. Seuraavassa käydään läpi yleisimpiä teorioita, kuinka yksityisyyttä on määritelty oikeuskirjallisuudessa. Näissä teorioissa yksityisyys nähdään omistettavana kohteena, muiden oikeuksien yhdistelmänä, kontrollivaltana tai asiana, jota suojellaan esteellä.

2.2.1. Yksityisyyden omistaminen ja muiden oikeuksien yhdistelmä

Aivan ensimmäinen teoria oli Warrenin ja Brandeisin ytimekäs määrittely: oikeus yksityisyyteen tarkoittaa oikeutta tulla jätetyksi rauhaan.[18] He johtivat perusteet oikeudelle yksityisyyteen analogisesti immateriaalioikeuksista ja omistusoikeudesta. Immateriaalioikeuden mukaan vain teoksen tai muun tuotoksen luojalla on oikeus päättää sen julkaisemisesta. Kyseinen julkaisuoikeus koskee tarkalleen ottaen teoksen taustalla olevaa ideaa ja ajatusta, ja näin tulisi olla vastaavasti myös yksityisten ajatusten ja ilmausten kohdalla. Niin ikään omistusoikeuden kohdalla ”yksilöllä on oikeus saada suojelua siihen, että yksinomaan hän saa käyttää ja nauttia siitä, mikä yksinomaan kuuluu hänelle”, minkä perusteella yksilön tulisi saada suojelua myös vain hänelle kuuluville yksityisille asioilleen.[19] Yksityisyyttä pidetään tässä teoriassa omistuksen kohteena, jonka piiriin kukaan ei saa tunkeutua ilman lupaa. Oikeus tulla jätetyksi rauhaan on kuitenkin aivan liian laaja toimiakseen ja toisaalta yksityisyyden loukkaus voi tapahtua, vaikka yksilö olisikin jätetty rauhaan. [20]

Nykyinen käsitys yksityisyydestä on edelleen hyvinkin yhtenevä omistusoikeuden kanssa.[21] Samoin kuin immateriaalioikeuksissa ei yksityisyydessä ole varsinaista konkreettista omistuksen kohdetta. Oikeudella yksityisyyteen tosin suojataan nimenomaan henkilöä, kun taas immateriaalioikeuksissa suojan kohde on idea, jota vain sen luoja voi käyttää ja hyödyntää. Yksityisyyden hahmottaminen omistusoikeuden kautta ei kuitenkaan toimi. Ensinnäkään se ei selitä, mitä yksityisyys on. Siten on epäselvää, mitkä asiat omistusoikeuden piiriin kuuluisivat. Yksityisyyden omistaminen olisi muutenkin hyvin poikkeavaa verrattuna perinteiseen omistusoikeuteen, sillä kun yksityinen asia on kerran tullut jonkun tietoon, ei sitä saa pyyhittyä ihmisten mielistä enää pois.[22] Yksityisyyden yksi ehkä ongelmallisimmista piirteistä on, että se voidaan periaatteessa menettää vain kerran eikä sen palaut-

[17] Rickless 2007, s. 779–780.
[18] Warren — Brandeis 1890, s. 193 ”the right to be let alone”.
[19] Warren — Brandeis 1890, s. 200–203, ja s. 205. “A man is entitled to be protected in the exclusive use and enjoyment of that which is exclusively his.” (Käännös tässä.)
[20] Parker 1974, s. 276.
[21] Allen 1999, s.724, ja Solove 2009, s. 26.
[22] Näin myös Solove 2009, s. 27.

taminen onnistu samoin kuin esimerkiksi varastetun tavaran. Omistusoikeudesta ei saadakaan johdettua mitään suojaa yksityisyyden loukkauksia vastaan.[23]

Vaikka omistusoikeus ei pysty yksinään selittämään oikeutta yksityisyyteen, reduktionistisen lähestymistavan mukaan omistusoikeus voisi olla osa sitä. Hohfeldin oikeuksista luoman mallin mukaan oikeudelle on olemassa neljä eri kategoriaa: väite, etuoikeus, valta ja immuniteetti. Näitä perustavanlaatuisia oikeuksia ei voida enää palastella pienemmiksi osasiksi ja ne toimivat peruspilareina monimutkaisemmille yhdistelmäoikeuksille.[24] Oikeus yksityisyyteen voidaan hahmottaa ensinnäkin yksinkertaisimmin väitteenä, ettei muilla ole pääsyä yksityisyyden piiriin ilman lupaa. Vaihtoehtoisesti sitä voidaan pitää yhdistelmänä etuoikeudesta, eli päätäntävallasta omista henkilökohtaisista tiedoista, ja väitteestä muita vastaan, etteivät he saa puuttua kyseiseen etuoikeuteen.[25]

Oikeus yksityisyyteen voidaan määritellä vielä monitahoisemmaksi yhdistelmäoikeudeksi niin, että sen katsotaan koostuvan omistusoikeudesta ja oikeudesta päättää omasta itsestään ja kehostaan. Nämä molemmat osaoikeudet ovat jo itsessään yhdistelmäoikeuksia, joten oikeus yksityisyyteen muodostuu osaoikeuksien pyramidiksi.[26] Reduktionistisella lähestymistavalla voidaan välttää yksityisyyden määrittelyn ongelma, sillä siinä oikeus yksityisyyteen perustuu muille fundamentaalisimmille oikeuksille eikä määritelmää siten tarvita. Reduktionisteilla ei kuitenkaan ole perusteita, miksi ajatuskulku menisi heidän väittämäänsä suuntaan, sillä voihan olla, että nämä fundamentaalisimpina pidetyt oikeudet juontavatkin juurensa oikeudesta yksityisyyteen eikä toisin päin.[27]

Siinä mielessä reduktionistit ovat ainakin oikeassa, että yksityisyys on jaoteltavissa eri osiin. Jo normeista on havaittavissa, että yksityisyyden suojan tarkennetaan kohdistuvan esimerkiksi perhe-elämään tai kirjeenvaihtoon, mutta nämä alakategoriat eivät ole Hohfeldin teorian mukaisia peruspilareita. Eri kategorioiden perusteella oikeuden yksityisyyteen voidaan osoittaa olevan sekä negatiivinen että positiivinen oikeus. Oikeuden negatiivista ulottuvuutta kuvaa esimerkiksi kirjesalaisuuden kohdalla valtion pidättäytyminen lukemasta kansalaistensa kirjeitä ja viestejä. Positiivinen ulottuvuus ilmenee puolestaan esimerkiksi

[23] Blume 2002, s. 26.
[24] Twining 2009, s. 50 ja Rickless 2007, s. 775, ”cluster-rights”.
[25] Rickless 2007, s. 779.
[26] Thomson 1975, s. 306.
[27] Inness 1992, s. 36.

siinä, että Suomessa kirjeeseen kajoaminen on kriminalisoitu (RL 38:3 viestintäsalaisuuden rikkominen) eli valtio tarjoaa kansalaisilleen suojaa oikeudenloukkaukselta.

2.2.2. Esteteoria ja yksityisyys kontrollina

Vastoin reduktionistien näkemystä, yksityisyyttä voidaan pitää myös kokonaisuutena, jota ei voida pilkkoa osaoikeuksiin. Yksityisyys olisi siten enemmän kuin Hohfeldin teorian mukaisten osaoikeuksien kokonaisuus. Niin sanotussa esteteoriassa yksityisyyttä itsessään ei yritetä määritellä, vaan sitä lähestytään sen kautta, miten yksityinen asia on pyritty suojaamaan. Esteteorian mukaan yksityistä asiaa suojaamassa täytyy olla jokin este, ja vasta se ylittämällä kyse on yksityisyyden loukkauksesta. Oikeus yksityisyyteen tämän näkökulman mukaan tarkoittaa sitä, että yksilö voi kieltää muita ylittämästä estettä ja sitä kautta estää heitä saamasta tietoonsa yksityisiä asioita, joita esteellä suojataan.[28]

Yksityisyyden määritelmä ei aiheuta tässä teoriassa hankaluuksia. Ongelma onkin siirretty vain eteenpäin, sillä yksityisyys määrittyy esteen kautta. Jos esteellä suojataan tietoja, jotka eivät yleisen käsityksen mukaan ole yksityisiä, ne tulisivat yksityisiksi esteen asettamisen seurauksena. Tätä epäloogisuutta voidaan hälventää harmillisuusperiaatteen avulla. Sen mukaan oikeuden ankaruus ja tiukkuus riippuvat siitä, kuinka paljon yksityisyyden loukkaus aiheuttaisi harmia loukkauksen kohteelle eli kuinka vakava loukkaus on.[29] Tässä kohtaa loukkauksen vakavuudelle tulisi määrittää objektiivinen mittapuu, sillä muutoin se perustuu vain subjektiiviseen yksityisyyden kokemiseen. Toinen ongelma teoriassa on se, että este käsitetään liian laajana. Esteen ei tarvitse olla täydellisen läpäisemätön, sen on voinut asettaa joku muu kuin kohde itse ja kohteen ei ole edes tarvinnut tarkoittaa sitä yksityisyyden suojaksi.[30] Rajanveto siitä, milloin kyse on yksityisyyttä suojaavasta esteestä, on siten hyvin epämääräistä, jos esteen ei edes tarvitse olla tarkoitettu yksityisyyden suojaamiseen.

Esteteoriassa yksilöllä on tietynlainen kontrolli yksityisyyteensä, jota hän hallitsee esteen avulla. Oikeutta yksityisyyteen usein pidetäänkin yksilön kontrollointivaltana. Kontrollivalta voi kohdistua esimerkiksi joko itseään koskeviin yksityisiin tietoihin tai tietojen sijaan niihin pääsystä päättämiseen.[31] Idea on, että yksityisyyttä ei omisteta, vaan sitä kontrollivallan kautta hallitaan. Ajatusta yksityisyydestä kontrollina voidaan kritisoida, sillä jo

[28] Rickless 2007, s. 787.
[29] Rickless 2007, s. 792–793.
[30] Rubel 2007, s. 803–805.
[31] Parker 1974, s. 281 ja Rickless 2007, s. 774.

uhka mahdollisesta yksityisyyden suojan loukkauksesta voi tarkoittaa oman kontrollin menetystä. Näin on esimerkiksi silloin, kun jonkun tiedetään omistavan laitteen, jolla saataisiin selville kaikki, mitä kohde kotonansa tekee.[32] Vaikka laitetta ei koskaan laitettaisi päälle, vaikuttaisi sen olemassaolo kuitenkin niin, että kohde ei enää voisi kontrolloida, mitä tietoja hän itsestään antaa ja kenelle. Siten pelkkä mahdollisuus oikeudenloukkaukseen olisi yksityisyyden loukkaus, mitä kontrolliteorioita vastustavat eivät hyväksy.[33]

Tilanne, jossa yksityistä keskustelua nauhoitetaan, muttei koskaan kuunnella,[34] on ainakin Suomessa katsottu yksityisyyden rikkomiseksi, sillä RL 24:5.1:n mukaan jo pelkkä tallentaminen on riittävää rikoksen tapahtumiseksi. Samoin on salakatselun kohdalla (RL 24:6), sillä siihenkin riittää kuvaaminen ilman, että kuvia tai videota koskaan katsottaisiin. Näissä tilanteissa uhri on menettänyt oman kontrollinsa yksityisyyteen, joten kontrolliteorialle voidaan löytää kannatusta Suomen lainsäädännöstä. Sekä salakuuntelun että -katselun valmistelu on myös kriminalisoitu (RL 24:7). Tällaisessa tilanteessa kontrollia ei ole menetetty, mutta se on heikentynyt uhan takia. Myös YK:n ihmisoikeuksista vastaava korkea edustaja on todennut, että ”jo pelkkä mahdollisuus siihen, että tietoa kommunikaatiosta voidaan kerätä, on yksityisyyden loukkaus”, mikä vastaa myös EIT:n näkökantaa.[35] Kontrolliteoria onkin vallitseva näkökulma yksityisyyteen.[36]

Kaikenkattavaa teoriaa ja määritelmää yksityisyydelle on mahdotonta antaa, sillä pelkästään julkisen ja yksityisen tiedon välinen rajanveto on vaikeaa. Mikä toiselle on yhdentekevää julkistaa, voi toiselle olla hyvinkin yksityistä. Kukin teoria toimii yhdessä kontekstissa, muttei välttämättä toisessa. Tämän perusteella Solove on tullut lopputulokseen, että oikeudessa yksityisyyteen kyse on pluralistisesta oikeudesta, joka koostuu toisiaan muistuttavista mutta silti erillisistä osista — aivan kuten perheenjäsenet muistuttavat toisiaan. Näin ollen oikeuteen yksityisyyteen kuuluu hyvin erilaisia alakategorioita, ja ne tekevät yksityisyyden kaikenkattavasta selittämisestä mahdotonta.[37]

[32] Thomson 1975, s. 305.
[33] Rickless 2007, s. 783.
[34] Ks. Rickless 2007, s. 790.
[35] YK A/HRC/27/37, kohta 20. “Even the mere possibility of communications information being captured creates an interference with privacy.” (Käännös tässä.)
Ks. myös EIT:n tuomiot Weber ja Saravia v. Saksa, kohta 78, Klass ja muut v. Saksa, kohta 41 sekä Malone v. UK, kohta 64. Tapaukset liittyvät viranomaisten mahdollisuuteen seurata yksityisiä ihmisiä ja kerätä heistä tietoa, mutta teorian kannalta eroa ei tulisi olla, onko kyse horisontaalisesta vai vertikaalisesta suhteesta.
[36] Solove 2009, s. 24.
[37] Solove 2009, s. 171–173.

2.2.3. Henkilötietojen suojan määrittely

Yksityisyyden yhtenä perheenjäsenenä pidetään usein henkilötietojen suojaa. Henkilötietojen suojan määrittely ei ole lainkaan niin mahdotonta kuin yksityisyyden, sillä suojan kohde eli henkilötiedot ovat määriteltävissä konkreettisesti. Henkilötiedot ymmärretään hyvin laajasti, sillä niitä ovat kaikki tiedot, joista luonnollinen henkilö voidaan tunnistaa. TSA 4(1) artiklan mukaan henkilötiedoilla tarkoitetaan

> *”kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä ’rekisteröity’, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella”.*

Kuten henkilötietojen myös niiden käsittelyn määritelmä on hyvin laaja. Oikeastaan kaikki toiminta, jossa henkilötiedot ovat jollakin tavalla osallisena, kuuluu henkilötietojen käsittelyn piiriin.[38] Henkilötietojen käsittelyllä TSA 4(2) artiklan mukaan tarkoitetaan

> *”toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista*”.

Etenkin henkilötietojen kohdalla edellä puhuttu yksityisyyden omistusoikeusnäkökulma voidaan ymmärtää hyvin; yksilö toimisi omien tietojensa omistajana.[39] Ajatus omistamisesta ei henkilötietojenkaan kohdalla kuitenkaan toimi, sillä henkilötietojen omistusoikeudesta ei voida edes luopua. Kun henkilötietojen käyttö sallitaan, tiedot saavasta tahosta ei voi tulla ainoa, jolla olisi täysi disponointivalta luovutettuihin tietoihin. Tällöinhän henki-

[38] Kulk – Zuiderveen Borgesius 2014, s. 390.
[39] Blume 2002, s. 25.

lötietojen kohde ja alkuperäinen omistaja ei voisi luovuttaa niitä enää toisille tahoille, kun taas uusi omistaja päättäisi täysin niiden käytöstä.

Henkilötietojen luovutuksessa samat tiedot pysyvät edelleen myös niiden aiemmalla ”omistajalla”, mikä tuo lisää ongelmia omistusoikeusnäkökulmaan. Nykyisin useat periaatteessa ilmaiset palvelut toimivat henkilötietojen luovuttamista vastaan,[40] joten henkilötiedot toimivat eräänlaisena valuuttana. Yritykset taas pitävät saamiansa tietoja omaisuutenaan ja liikesalaisuutena.[41] Tämä lisää houkutusta ajatella henkilötietoja omistettavina, mutta toisin kuin perinteistä rahaa, henkilötietojaan voi luovuttaa rajattomasti uudestaan ja uudestaan myös toisille tahoille. Jos henkilötietoja pidettäisiin omistettavina, tietojenluovuttamisen seurauksena syntyisi valtava vyyhti yhteisomistajuutta. Tällöin omien tietojensa luovuttaja ei voisi luopua omistuksestaan, ja niiden vastaanottajat voisivat vain osittain päättää niiden käytöstä siihen asti, kunnes tietojen kohde saattaisi vaatia heitä poistamaan henkilötiedot rekisteristä eli luopumaan niiden omistuksesta. Kyse ei ole siten omistuksesta. Tätä puoltaa sekin, ettei rekisteröity voi aina edes itse estää tietojensa käsittelyä.[42]

Edellä mainitusta havaitaan, ettei esteteoriakaan ei toimi henkilötietojen suojan kohdalla. Jos rekisteröity ei voi itse estää henkilötietojensa laillista käsittelyä, on yhdentekevää, minkälaisilla esteillä hän yrittäisi henkilötietojaan suojata. Lisäksi monet henkilötiedoista, kuten nimi, ovat mahdottomia asettaa esteen taakse, jolloin kyseiset tiedot eivät nauttisi henkilötietojen suojaa esteen puuttumisen takia. Puolestaan reduktionistisen käsityksen mukaisesti henkilötietojen suojan voitaisiin katsoa koostuvan esimerkiksi rekisteröidyn etuoikeudesta päättää omista henkilötiedoista ja väiteoikeudesta muita vastaan, etteivät he puutu tämän etuoikeuden käyttämiseen. Tosiasiassa etuoikeuden käyttämiseen voidaan kuitenkin puuttua rekisteröidyn vastustuksesta huolimatta. Samoin törmätään samaan ongelmaan, joka tuli jo yksityisyyden kohdalla esiin. Miten Hohfeldin teoriassa fundamentaalisimpien oikeuksien voidaan tosiasiassa osoittaa olevan perustavanlaatuisimpia? Mahdollistahan on, että vasta oikeuksien yhdistelmä, kuten henkilötietojen suoja, tekee näistä oikeuksista tärkeitä ja perustavanlaatuisia.

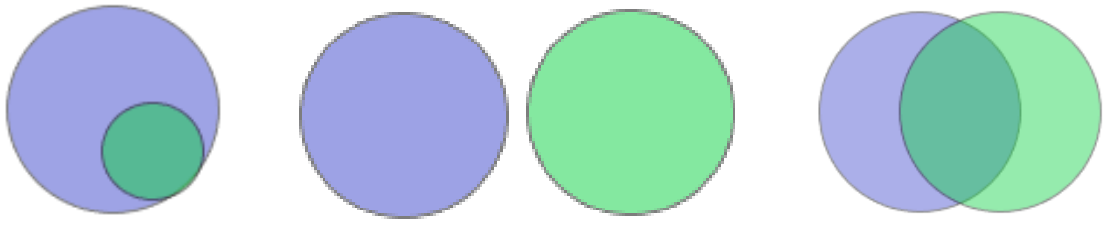
Kaikissa edellä kuvatuissa tilanteissa on viitteitä rekisteröidyn kontrollivaltaan, mikä on henkilötietojen suojassa nähdäkseni luontevin lähestymistapa. POK 8(2) artiklasta ilmenee, henkilötietojen suojalla tarkoitetaan henkilötietojen lainmukaista ja oikeasuhtaista käsitte-

[40] Esimerkiksi sosiaalisen median palvelut kuten Facebook ja Instagram.
[41] Blume 2002, s. 26.
[42] de Hert — Gutwirth 2009, s. 3.

lyä siten, että rekisteröidyllä on lähtökohtaisesti mahdollisuus kontrolloida käsittelyä tai tietoja. Yleisenä suuntauksena on, että mitä enemmän teknologia, tietojen keruu sekä niiden käsittely kehittyvät, sitä suurempi mahdollisuus halutaan antaa rekisteröidyille kontrolloida heitä koskevia tietoja.[43] Kontrollin avulla yksityishenkilö voi varjella julkista mainettaan ja kunniaansa. Henkilötietojen suoja, yksityisyys sekä yksilön kunnia linkittyvätkin vahvasti toisiinsa.[44] Kontrollissakin kyse on kuitenkin vain lähtökohdasta, sillä henkilötietoja voidaan käsitellä myös muilla oikeusperusteilla kuin rekisteröidyn antamalla suostumuksella. Henkilötietojen suoja ei tarkoita samanlaista asioiden piilottamista tai salassapitoa kuin yksityisyys, vaan se voi johtaa itse asiassa läpinäkyvyyteen.[45] Tätä voidaan jossain kohtaa jopa pitää yksityisyyden vastakohtana, joten seuraavaksi on tarpeen selventää henkilötietojen suojan ja oikeuden yksityisyyteen välistä suhdetta. EU:ssa henkilötiedoille on annettu perusoikeussuoja erillisenä yksityisyydestä, ja niiden välisestä suhteesta on eriäviä mielipiteitä.

2.2.4. Yksityisyyden ja henkilötietojen suojan välinen suhde

Yksityisyyden ja henkilötietojen suojan välinen suhde voidaan hahmottaa kolmella eri tavalla. Ensinnäkin henkilötietojen suojan voidaan katsoa olevan yksityisyyden alakategoria. Toiseksi niitä voidaan pitää toisistaan täysin erillisinä oikeuksina. Kolmas vaihtoehto on edellisten yhdistelmä siten, että oikeus yksityisyyteen ja henkilötietojen suoja ovat toisistaan erilliset mutta toisiaan täydentävät.[46] Alla olevat kuvat kuvastavat näitä eri lähtökohtia. Sininen ympyrä on oikeus yksityisyyteen ja vihreä ympyrä puolestaan henkilötietojen suoja. Ensimmäisessä kuvassa henkilötiedot kuuluvat yksityisyyteen täysin, toisessa ne ovat toisistaan erilliset oikeudet, ja kolmannessa oikeudet leikkaavat toisiaan, mutta niillä on myös omat, erilliset alueensa.



[43] Ks. Euroopan neuvoston päätös 1196, kohta 5.
[44] Hijmans 2016, s. 46 ja WP 225, s. 16.
[45] Forde 2016, s. 138.
[46] Lynskey 2015, s. 90.

Oikeus yksityisyyteen ja oikeus henkilötietojen suojaan ovat helposti sekoitettavissa keskenään, mutta kyse on mielestäni eri asioista. Yleensä henkilötietojen käsittelyssä tietosuojanormit tulevat automaattisesti sovellettavaksi, mutta sääntely yksityisyydestä aktivoituu vasta, kun tilanteessa on kyse myös oikeudesta yksityisyyteen, ja toisinpäin.[47] Erojakin on. Esimerkiksi Iso-Britanniassa henkilötietojen suoja on vain osa yksityisyyttä eikä tietosuojanormeja sovelleta, ellei kyse ole samalla oikeudesta yksityisyyteen.[48] Suomessa oikeuden yksityisyyteen takaavaan PL 10 §:ään on otettu mukaan myös henkilötietojen suoja, joten lainsäätäjä on niputtanut kyseiset oikeudet yhteen. Lainsäätäjän tarkempaa ajatusta niiden suhtautumisesta toisiinsa ei kuitenkaan PL 10 §:n perusteella voida tehdä.

Yksityisyydellä on hyvin merkittävä rooli tietosuojan suhteen, ja tietosuojanormeilla pyritäänkin ensisijaisesti turvaamaan yksilön oikeus yksityisyyteen, mutta se ei ole tietosuojanormien ainoa tavoite ja tarkoitus.[49] Esimerkiksi EU:n tietosuojalainsäädännön tavoitteena on myös sisämarkkinoiden yhdentäminen sekä tehokas tietojen siirto jäsenvaltioiden välillä,[50] jolloin yksittäinen jäsenvaltio ei voi vaatia tietosuoja-asetuksessa säädetystä parempaa henkilötietojen suojaa omalla alueellaan. Periaatteessa myöskään rekisteröidyn oikeudessa saada tietää, mitä tietoja hänestä on rekisterissä, ei ole kyse yksityisyyden suojasta vaan kontrollin antamisesta. Vasta sitten kun rekisteröity voi vaatia muutoksia tietoihin tai niiden poistoa, yksityisyys voi tulla kyseeseen tapauksesta riippuen. Samoin rekisteröidyn oikeus tietojensa siirtoon toisesta rekisteristä toiseen antaa rekisteröidylle päätäntävaltaa omien tietojensa käytöstä, mutta sillä ei varsinaisesti ole mitään tekemistä yksityisyyden kanssa — ellei rekisteröidyn syy siirtoon esimerkiksi perustu hänen kokemaansa yksityisyyden suojan uhkaan.

Liityntä henkilötietojen suojan ja oikeuden yksityisyyteen välillä on silti hyvin selkeä ja kiinteä eikä yksityisyysaspektia voida milloinkaan kokonaan erottaa henkilötietojen suojasta. Henkilötietojen suojan käsittäminen yksityisyyden yhdeksi osa-alueeksi on ymmärrettävää. Henkilötietojen suoja tuskin olisi kehittynyt ilman oikeutta yksityisyyteen. Perusoikeuskirjassa niistä kuitenkin säädetään eri artikloissa: POK 7 artikla koskee oikeutta yksityisyyteen ja POK 8 artikla oikeutta henkilötietojen suojaan. Jos henkilötietojen suoja kuuluisi suoraan oikeuden yksityisyyteen alle, pitäisi POK 7 artiklan kattaa myös se, jolloin POK 8 artiklaa ei erikseen tarvittaisi. Erottelu heijastelee oikeuksien erillisyyttä ja poikke-

[47] Gellert — Gutwirth 2013, s. 526.
[48] Lynskey 2014, s. 572.
[49] WP 225, s. 16, ja Bygrave 2001, s. 282.
[50] TSA johdanto kohta 10, TSA 1 art.

aa kansainvälisistä ihmisoikeusdokumenteista, joissa henkilötietojen suojaa pidetään yleensä yksityisyyden alakategoriana.[51] Esimerkiksi EIS ei sisällä säännöksiä henkilötietojen suojasta, mutta oikeuskäytännössään EIT on katsonut EIS 8 artiklan takaaman oikeuden yksityisyyteen laajaksi ja sisällyttänyt siihen myös henkilötietojen suojan.[52]

Myös EUT on yhdistänyt oikeudet pitäen henkilötietojen suojaa oikeuteen yksityisyyteen kuuluvana.[53] Tuomioistuimen linjauksissa on kuitenkin ollut ajoittain eroja, kuinka henkilötietojen suoja ja yksityisyys suhtautuvat toisiinsa.[54] Perustelluinta on mielestäni pitää kyseisiä oikeuksia toisistaan erillisinä mutta toisiaan täydentävinä. Kaikki henkilötiedot eivät ole yksityisiä[55] samoin kuin kaikki yksityiset asiat eivät välttämättä ole henkilötietoja. Rajanveto ei ole aina selkeää, sillä yhdessä henkilötiedot ovat enemmän kuin osiensa summa. Yksittäisiä, ei-yksityisiä henkilötietoja voidaan yhdistellä, jolloin tietojen kokonaisuus tai sitä analysoimalla saadut tiedot voivatkin olla yksityisiä tai arkaluonteisia. Silti henkilötieto, joka ei kuulu yksityisyyden piiriin, kuuluu henkilötietojen suojan piiriin. Henkilötietojen suoja ja oikeus yksityisyyteen siten leikkaavat toisiaan,[56] ja koska niiden välinen yhteys on niin kiinteä, ovat ne nykymaailmassa itse asiassa riippuvaisia toisistaan. Myös tapauksessa C-92/09 henkilötietojen suojan katsottiin liittyvän kiinteästi oikeuteen yksityisyyteen ilman, että henkilötietojen suojaa pidettiin osana yksityisyyttä.[57]

Päinvastaisen näkemyksen mukaan kyse olisi täysin erillisistä oikeuksista, jotka saattavat olla toisilleen jopa uhka. Esimerkiksi henkilötietojen suojaan kuuluva rekisteröidyn oikeus päästä omiin tietoihinsa vaarantaisi oikeuden yksityisyyteen. Rekisterinpitäjällä ei aina ole suoraa yhteyttä rekisteröityyn, vaan henkilötiedot on voitu saada kolmannelta taholta. Tällaisella rekisterinpitäjällä ei välttämättä ole mahdollisuutta luotettavasti varmistua tietojansa vaativan henkilöllisyydestä, mikä aiheuttaisi uhan yksityisyydelle, jos tietoja annetaankin väärälle henkilölle.[58] Tämä ei siltikään muodosta perustetta katsoa oikeuksien olevan vastakkaisia. Esimerkki osoittaa lähinnä, että niiden välillä voi olla jännitettä, mikä puhuu oikeuksien erillisyyden puolesta. Se ei kuitenkaan osoita, etteikö henkilötietojen tiivis ja kiinteä suhde olisi olemassa, jolloin todellista vastakkainasettelua ei ole. Kyse on lähinnä

[51] Lynskey 2014, s. 569–570.
[52] Kulk – Zuiderveen Borgesius 2014, s. 392, ja Gellert — Gutwirth 2013, s. 524.
[53] Lynskey 2014, s. 573, 581.
[54] Koillinen 2013, s. 178–180.
[55] WP 225, s. 16.
[56] Gellert — Gutwirth 2013, s. 526.
[57] C-92/09, kohta 47.
[58] Cormack 2016, s. 17, 24–26.

käytännön toteutuksesta. Henkilötietojen päätyessä vääriin käsiin rikotaan sekä tietosuojaa että mahdollisesti myös yksityisyyden suojaa, jos annetut tiedot ovat olleet yksityisiä

Jännite oikeuksien välillä on kiistatta olemassa. Tietosuojasääntelyllä yleensä pyritään yhdistämään sekä rekisteröidyn oikeus yksityisyyteen että rekisterinpitäjän perustellut intressit käsitellä henkilötietoja, mikä periaatteessa on uhka yksityisyydelle. Osapuolten intressit ovat helposti ristiriidassa keskenään, joten pyrkimällä ottamaan kummatkin asianmukaisesti huomioon voidaan niiden toteutuminen turvata henkilötietojen suojalla samalla tavalla kuin ympäristöoikeudessa kestävällä kehityksellä pyritään suojaamaan sekä ympäristöä että talouskasvua.[59] Henkilötietojen suoja palvelee siten useampaa päämäärää sovittamalla yhteen yksityisyyden suojan tietoyhteiskunnan, yritysten ja teknologian tarpeiden kanssa. Näin ollen oikeus yksityisyyteen ja oikeus henkilötietojen suojaan vetävät osittain samaan ja osittain eri suuntiin, joten kyseiset oikeudet eivät ole toisistaan täysin erilliset, mutta henkilötietojen suojaa ei myöskään voida pitää alisteisena oikeudelle yksityisyyteen. Tästä johtuen käsittelen henkilötietojen suojaa ja yksityisyyttä vahvasti toisiinsa kietoutuneina, sillä erillinen käsittely olisi mahdotonta. Mukaillen Soloven näkemystä yksityisyydestä eräänlaisena perheenä yksityisyys ja henkilötietojen suoja eivät ole perheenjäseniä vaan toistensa lähisukulaisia.

[59] Bygrave 2001, s. 282.

3. Yksityisyys ja henkilötietojen suoja ihmisoikeuksina

Edellä selvitettiin keskeisimpiä käsitteitä henkilötietojen suojasta ja yksityisyydestä. Seuraavaksi keskitytään henkilötietojen suojan ja oikeuden yksityisyyteen asemaan ihmisoikeutena, jotta mahdolliset erot etenkin EU:n ja muun maailman välillä tulisivat esille. Edellä on puhuttu lähinnä eurooppalaisesta lainsäädännöstä, jonka perusteella on ilmeistä, että oikeudella yksityisyyteen sekä henkilötietojen suojalla on vahva perus- ja ihmisoikeusasema EU:ssa. Koska tarkoituksena on selvittää EU:n mahdollista ekstraterritoriaalista vaikutusta niiden suhteen, tarpeen on tietää yksityisyyden ja henkilötietojen suojan asemasta muuallakin. Oikeuden yksityisyyteen ja henkilötietojen suojan ymmärtäminen ihmisoikeuksina on tärkeää, sillä EU:n yhtenä tavoitteena on juuri ihmisoikeuksien edistäminen globaalisti, mistä puhutaan tarkemmin neljännessä luvussa. Tämän luvun lopussa myös tarkastellaan yksityisyyden ja henkilötietojen suojan suhdetta sananvapauteen ja turvallisuuteen, sillä kokonaisvaltaisen kuvan saamiseksi on myös tiedettävä mahdollisista ristiriidoista muiden perusoikeuksien kanssa. Oikeuksien erilainen punninta toisiaan vastaan myös aiheuttaa eroja eri lainkäyttöpiirien välille. Tämä tulee hyvin esille EU:n ja Yhdysvaltojen välillä, mikä ilmenee tarkemmin viidennessä ja kuudennessa luvussa.

3.1. Oikeuden yksityisyyteen ja henkilötietojen suojan universaalius

3.1.1. Universaali ihmisoikeus

Oikeus yksityisyyteen on kirjattu YK:n ihmisoikeusjulistuksen 12 artiklaan. YK:n ihmisoikeuksien korkean edustajan mukaan oikeus yksityisyyteen on universaalisti tunnustettu ihmisoikeudeksi, sillä YK:n julistusten ja sopimusten lisäksi valtioiden kansallisissa laeissa suojataan yksityiselämää.[60] Yleensä nimenomaan YK:n ihmisoikeusjulistuksen nähdään olevan yleismaailmallinen lista arvoista ja oikeuksista, jotka ovat universaalisti kaikkialla maailmassa hyväksytty ja joita halutaan suojata.[61] Ihmisoikeusjulistuksen lisäksi lähes kaikki maailman valtiot ovat allekirjoittaneet ja ratifioineet KP-sopimuksen[62], jonka 17 artiklassa oikeus yksityisyyteen vahvistetaan kansainväliseksi sopimusvelvoitteeksi ja joka siten on velvoittavampi kuin ihmisoikeusjulistus. Näin ollen on perusteltua pitää oikeutta yksityisyyteen universaalina ihmisoikeutena.

[60] YK A/HRC/27/37, kohta 13.
[61] Twining 2009, s. 124.
[62] ks. http://indicators.ohchr.org/

Näin suoraviivaista johtopäätöstä ei kuitenkaan kannata tehdä, sillä edellä mainitut instrumentit ovat lähtökohdiltaan hyvin länsimaisia kuin myös näkemykset siitä, kuinka niitä tulisi soveltaa. Oikeuden yksityisyyteen universaalius voi ollakin vain ”pinnallista”. Tällöin sanamuoto on niin epämääräinen ja monitulkintainen, että kaikki ovat voineet hyväksyä sen.[63] Toisaalta valtioilla on yleensä mahdollisuus ilmoittaa varauksensa koskien tiettyjä sopimusten artikloja, jolloin niiden näkemykset ja kulttuuri voidaan huomioida tulkinnassa. Samalla sopimuksen sanamuodon merkitys tuodaan ilmi varauksen tehneen valtion kohdalla, mikä vähentää universaaliuden pinnallisuutta mutta samalla myös yhteisymmärrystä kyseisen oikeuden merkityksestä. Lisäksi varausten kohdalla rajat tulevat jossain kohtaa vastaan, ja yleensä varausten hyväksyttävyyttä tarkastellaankin länsimaisesta näkökulmasta.[64] Pohjois-Amerikka, Australia ja Euroopan jakavat samat länsimaiset arvot ja periaatteet vain pienin eroavaisuuksin, joten niissä oikeus yksityisyyteen on hyväksytty ihmisoikeudeksi YK:n näkemyksen mukaisesti. YK:n toimintaa usein pidetään länsimaisena,[65] joten sen julistukset ja sopimukset ovat sopusoinnussa kyseisten maiden näkemysten kanssa.

Kaikki Afrikan maat Etelä-Sudania lukuun ottamatta ovat ratifioineet KP-sopimuksen, mutta tästä huolimatta Afrikan unionin ihmisoikeuksien ja kansojen oikeuksien peruskirjassa ei ole lainkaan mainintaa yksityisyyden suojasta, vaikka se on laadittu YK:n ihmisoikeusjulistuksen ja KP-sopimuksen tekemisen jälkeen. Yksityisyyden ei ole siten katsottu tarvitsevan mitään erityistä suojaa. Verrattaessa länsimaiseen yksilöä korostavaan näkemykseen Afrikan maissa kulttuurit ovat huomattavasti yhteisöllisempiä, jota kuvastaa afrikkalainen Ubuntu-periaate. Sen mukaan yhteisö menee yksilön edelle eikä ihminen elä yksilönä itselleen vaan yhteisölle: Jokaisen tulisi pyrkiä kohti yhteisön hyvinvointia, sillä vain sitä kautta myös yksilöt voivat hyvin.[66] Koska ihmisyys ja yksilön individuaalisuus voi Ubuntun mukaan toteutua vain yhteisön kautta, ja läpinäkyvää ja avointa kulttuuria

[63] Twining 2009, s. 124 ja s. 129, “surface universalism”.
[64] Esimerkiksi Bahrainin kuningaskunta on tehnyt varaukset koskien KP-sopimuksen 3 artiklaa (samat oikeudet miehille ja naisille), 18 artiklaa (uskonnon- ja omantunnon vapaus) ja 23 artiklaa (oikeus avioliittoon ja sen vapaaehtoisuus) niin, että kyseiset artiklat eivät vaikuta Sharia-lain määräyksiin ja noudattamiseen. Monet länsimaat ilmoittivatkin vastustavansa varauksia, koska ne oli tehty myöhässä ja koska niillä kajottiin sopimuksen olennaisimpiin osiin. Myös KP-sopimuksen itsensä eli artiklan 4(2) mukaan artiklaan 18 ei voida tehdä mitään rajoituksia tai varauksia. Bahrainin hallituksella on selvästi hyvin erilainen käsitys ihmisoikeuksista kuin länsimailla.
(ks. https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_en)
[65] YK:n länsimaisuus ilmenee hyvin esim. turvallisuusneuvoston kohdalla. Sen päätökset sitovat kaikkia jäsenmaita, joten se on elimistä tärkein (ks. lisää http://www.yk.fi/node/227) ja sen pysyvistä viidestä jäsenestä kolme on länsimaata.
[66] Kwamwangamalu 1999, s. 27.

painotetaan, ei henkilökohtaisella, länsimaisen ajattelumallin mukaisella yksityisyydellä ole Ubuntu-ajattelussa juurikaan tilaa tai merkitystä.[67]

Edellä mainitusta huolimatta on joidenkin Afrikan maiden omissa perustuslaeissa turvattu oikeus yksityisyyteen,[68] ja lainsäädäntö yksityisyydestä on lisääntynyt eri puolilla Afrikkaa.[69] Ubuntun vaikutus oikeuteen ja yhteiskuntaan on kuitenkin merkittävää,[70] joten uusista laeista huolimatta on oletettavissa, että yksityisyys ymmärretään Afrikassa länsimaista poikkeavasti. Yksityisyydellä ei ole länsimaihin verrattuna lainkaan niin suurta painoarvoa, mikä syö sen asemaa perustavanlaatuisena ihmisoikeutena. Kuitenkin KP-sopimuksen ratifioinnin sekä uusien lakien perusteella oikeuden yksityisyyteen voidaan katsoa olevan hyväksytty ihmisoikeudeksi myös Afrikassa, mutta heikommalla painotuksella.

Latinalaisen Amerikan kulttuurit ovat lähempänä länsimaita kuin esimerkiksi afrikkalaiset, joten näkemyserot oikeudesta ovat siten pienemmät. Bogotan julistuksen 5 artikla ja tämän jälkeen laaditun Amerikan ihmisoikeussopimuksen 11 artikla sääntelevät oikeudesta yksityisyyteen. Niiden mukaan jokaisen kunniaa ja ihmisyyttä tulee kunnioittaa, ja yksityis- ja perhe-elämä sekä koti ja kirjeenvaihto on suojattu mielivaltaiselta tai loukkaavalta kajoamiselta. Ilmaus on hyvin yhtenevä EIS:n ja KP-sopimuksen kanssa, joten oikeus yksityisyyteen ja ihmisoikeusasema hahmotetaan latinalaisessa Amerikassa samansuuntaisesti kuin länsimaissa.

Islamilainen maailma on usein napit vastakkain länsimaisten arvojen ja periaatteiden kanssa, ja esimerkiksi lähes mikään Arabian niemimaan valtioista ei ole ratifioinut KP-sopimusta. Islamilaisen näkemyksen mukaan länsimaiset ihmisoikeudet perustuvat sekulaareille arvoille, kun taas islamilaiset ihmisoikeudet ovat jumalallista alkuperää, minkä perusteella esimerkiksi Iran on jättänyt noudattamasta kansainvälisiä ihmisoikeusvelvoitteitaan.[71] Muslimimailla on oma ihmisoikeusjulistuksensa — Kairon julistus ihmisoikeuksista islamissa eli Kairon ihmisoikeusjulistus — jonka 18 artiklassa on turvattu oikeus yksityisyyteen. Julistuksen artiklojen tulkinnan on tapahduttava Sharia-lain mukaisesti,[72] minkä tähden eroavuudet verrattuna länsimaiseen näkemykseen yksityisyydestä ovat hyvin

[67] Olinger et al. 2007, s. 31–43 (ei sivunumerointia).
[68] Esim. Etelä-Afrikan perustuslain 14 art., Etiopian perustuslain 26 art. ja Kongon demokraattisen tasavallan perustuslain 31 art.
[69] Makulilo 2012, s. 168–169.
[70] Olinger et al. 2007, s. 31–43 (ei sivunumerointia).
[71] Ali 2000, s. 25–26.
[72] Kairon ihmisoikeusjulistuksen artiklat 24 ja 25.

todennäköisiä. Tästä huolimatta yksityisyydelle on haluttu antaa suojaa muslimimaissakin, mikä puoltaa oikeuden universaalia luonnetta. Kyse on tosin julistuksesta, joten sen velvoittavuus on heikompaa kuin sopimusten.

Aasian osalta ASEAN-maiden ihmisoikeusjulistuksen 21 artiklassa suojataan oikeus yksityisyyteen ja samassa artiklassa erikseen mainitaan myös henkilötiedot. Julistuksen tarkoituksena on ollut vahvistaa YK:n ihmisoikeusjulistus, YK:n perusoikeuskirja ja muita kansainvälisiä ihmisoikeussopimuksia ja -instrumentteja.[73] Julistuksen 7 artiklassa kuitenkin todetaan, että ihmisoikeuksien toteutumisessa on otettava huomioon alueellinen ja kansallinen konteksti huomioiden myös poliittiset, taloudelliset, oikeudelliset, sosiaaliset, historialliset ja uskonnolliset taustat.[74] Vaikka samassa kohdassa ihmisoikeuksien todetaan olevan universaaleja, niiden tulkinnassa ja toteuttamisessa halutaan kuitenkin käyttää omaa, paikallista mittapuuta. Siten käsitys yksityisyydestä ja sitä kautta myös henkilötietojen suojasta ja sen tarpeellisuudesta voi poiketa paljonkin länsimaisesta näkemyksestä. Aasian kulttuureissa ”kasvojen säilyttäminen” on tärkeää, joten yksityisinä saatetaan pitää tietoja, jotka esimerkiksi Euroopassa eivät aiheuttaisi ongelmia. Toisaalta myös yhteisöllisyys on vahvempaa, minkä seurauksena yksilöä ja hänen oikeuksiaan tarkastellaan enemmän yhteisön ja yhteiskunnan tarpeista käsin.

Edellä esitetyn perusteella havaitaan, että oikeus yksityisyyteen on kirjattu moniin sopimuksiin ja julistuksiin Afrikan perusoikeuskirjaa lukuun ottamatta. Kuten sanottua, afrikkalaisissakin perustuslaeissa yksityisyys on kuitenkin huomioitu ja tietosuojalainsäädännön lisääntyessä suuntauksena on yksityisyyden merkityksen kasvu myös Afrikassa. Yksityisyyden luonteesta ja kulttuurisidonnaisuudesta johtuen käsitys yksityisyydestä vaihtelee väkisinkin.[75] Kuten Solove asian ilmaisee, ”yksityisyys on tila, jonka itse luomme, ja sellaisena se on dynaaminen ja muuttuva”.[76] Kovin suuret tulkintaerot ihmisoikeuksien kohdalla eivät yleensä ole mahdollisia. Toimet, jotka rikkovat oikeutta elämään Euroopassa, rikkovat sitä myös muualla. Yksityisyys ja henkilökohtaisina tietoina pidettävät asiat riippuvat kuitenkin sekä yksilön subjektiivisista näkemyksistä että hänen kulttuuristaan ja kyseisen kulttuurin muokkaamasta yhteiskunnasta, jossa hän elää.[77] Siten yksityisyyden ja

[73] ASEAN-maiden ihmisoikeusjulistuksen esipuheen 3. kohta.
[74] “At the same time, the realisation of human rights must be considered in the regional and national context bearing in mind different political, economic, legal, social, cultural, historical and religious backgrounds.”
[75] Himma 2007, s. 864.
[76] Solove 2009, s. 65. “Privacy is a condition we create, and as such, it is dynamic and changing.” (Käännös tässä.)
[77] Solove 2009, s. 50.

henkilötietojen kohdalla tilanne on poikkeuksellinen ihmisoikeuksien näkökulmasta. Se, että oikeus yksityisyyteen on haluttu ympäri maailmaa ottaa sopimuksiin ja julistuksiin mukaan, osoittaa, että mahdollisista tulkinta- ja painotuseroista huolimatta ihmiskunta kokonaisuudessaan haluaa suojaa yksityisinä pitämilleen asioille. Tämän perusteella katson, että yksityisyyttä ja sitä kautta myös henkilötietojen suojaa voidaan pitää universaalina ihmisoikeutena mahdollisista näkemyseroista huolimatta.

Ihmisoikeuksien universaalius kiistetään usein väittämällä, että kyse olisi vain länsimaisista arvoista. Kuitenkin jokainen valtio on lähtökohtaisesti suvereeni, minkä takia myös edellä puhutuille YK:n ihmisoikeusdokumenteille annetulla hyväksynnällä on merkitystä. YK:n jäsenet ovat suvereeneina valtioina itse päättäneet liittymisestään ja allekirjoittamalla YK:n peruskirjan ne ovat myös hyväksyneet ihmisoikeusjulistuksen, joten syytökset esimerkiksi ihmisoikeusjulistuksen länsimaisuudesta vaikuttavat liioitelluilta. Toisaalta nykyisessä globaalissa maailmassa täydellinen erillisyys muista valtioista on mahdotonta, joten YK:n jäsenenä oleminen on valtiolle lähes välttämätöntä. Pieniä kiistanalaisia alueita lukuun ottamatta lähes kaikki maailman valtiot kuuluvatkin siihen. Ongelma ei kuitenkaan nähdäkseni ole se, että ihmisoikeuksia ei yleisesti hyväksyttäisi, vaan se, että valtioiden johtajat eivät halua toteuttaa niitä, koska parantamalla kansalaistensa asemaa heidän etuoikeutensa ja valtansa todennäköisesti pienenisi.

Kansainvälisissä sopimuksissa tai ihmisoikeusjulistuksissa puhutaan oikeudesta yksityisyyteen, mutta mainintaa henkilötietojen suojasta ei löydy. Sen takia onkin muistettava eri näkemykset yksityisyyden ja henkilötietojen suojan välisestä suhteesta, jota käsiteltiin edellisen luvun lopussa. Kansainvälisissä ihmisoikeusdokumenteissa henkilötietojen suoja hahmotetaan kuuluvan oikeuden yksityisyyteen alle.[78] Sen takia henkilötietojen suojaa on tarkasteltava tässä kohtaa oikeuden yksityisyyteen alakategoriana, vaikka edellä katsoinkin oikeuksien olevan erillisiä mutta kuitenkin toisiinsa kiinteästi sidoksissa. Lähestymistavat ovat lähellä toisiaan, ja suhde oikeuksien välillä on niin kiinteä, että on selvää, että myös henkilötiedoille annetaan suojaa, mikäli yksityisyyttä halutaan suojata. Muuten oikeus yksityisyyteenkään ei toteutuisi. Siten vaikka erillistä mainintaa henkilötietojen suojasta ei aina ole, myös henkilötietojen suoja käsitetään ihmisoikeudeksi. Euroopan neuvosto on

[78] Lynskey 2014, s. 569–570.

lisäksi tehnyt henkilötietojen suojasta erillisen sopimuksen, jossa se vahvistaa henkilötietojen suojan ihmisoikeusaseman.[79]

Yksityisyyden kulttuurisidonnaisuuden ja puuttuvan määritelmän perusteella on myös esitetty vastakkaisia näkemyksiä, ettei yksityisyyden suoja olisi universaalisti hyväksytty tai ettei universaaliudelle olisi edes tarvetta, kuten Westin on katsonut.[80] Westin näkemys on nykymaailmassa vanhentunut, sillä internetin takia olisi hyvä olla edes jonkinlainen yhteisymmärrys yksityisyydestä ja henkilötietojen suojasta, koska internet ulottuu kaikkialle, minne yhteyttä rakennetaan. YK:n mukaan oikeuksien, jotka yksilöllä on offline-tilassa eli konkreettisessa maailmassamme, täytyy olla voimassa myös ihmisen ollessa online-tilassa eli internetin virtuaalisessa maailmassa.[81] Oikeus yksityisyyteen ja henkilötietojen suoja ulottuu siten myös internetiin. Internetin myötä on syntynyt virtuaalimaailma, joka on samaan aikaan kaikkien valtioiden oikeudenkäytön alla ja samalla ei-kenenkään-maata, mikä aiheuttaa ristiriitoja, jos konsensusta internetissä olevista oikeuksista ja niiden toteuttamisesta ei ole.

3.1.2. Rikkaiden oikeus?

1800-luvulla ja sitä ennen yksityisyys oli vain rikkaiden ylellisyyttä. Tämä sama tilanne, joka ennen vallitsi alueellisesti, vallitsee nykyisin globaalisti.[82] Rikkaammissa länsimaissa yksityisyyden suoja on vahvempi kuin kehittyvissä maissa, mutta toisaalta näin on myös muidenkin ihmisoikeuksien kohdalla. Upendra Baxi näkee ihmisoikeuksien tulleen kauppatavaraksi ja joutuneen vahvempiin käsiin, niin että ihmisoikeudet ovat menettäneet alkuperäisen tarkoituksensa, joka on suojata köyhiä ja sorrettuja.[83] Onko yksityisyys ja henkilötietojen suoja siten nykyäänkin vain rikkaiden oikeus, vaikka ne olisi universaalisti hyväksytty?

Rikkaissa maissa teknologiaa käytetään entistä enemmän ja laadullisesti kehittyneemmin, mikä mahdollistaa ihmisistä tiedon keräämisen tehokkaasti ja samalla yksityisyyden ja henkilötietojen suojan loukkaamisen helpommin. Tällä perusteella länsimaisella ihmisellä olisi huomattavasti enemmän uhkia joutua yksityisyyden loukkauksen uhriksi kuin hei-

[79] Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data.
[80] Blume 2002, s. 15 ja Solove, s. 66, viittaus Alan Westin: Privacy and Freedom. London 1967, s. 12.
[81] YK 68/167, kohta 3.
[82] Blume 2002, s. 9–10.
[83] Twining 2009, s. 177.

monsa kanssa perinteisesti, keskellä viidakkoa elävällä alkuasukkaalla. Tämä on kuitenkin vanhentunut stereotyyppinen ajatus kehitysmaista, sillä suurin osa kehittyvien maiden ihmisistä ei elä keskellä viidakkoa ilman yhteyttä muuhun yhteiskuntaan. Samalla tavalla uusi teknologia lisääntyy kehittyvissä maissa, joten yksityisyyden suojan uhat ovat siellä samat kuin länsimaissakin — elleivät jopa suuremmat mahdollisesti puutteellisen lainsäädännön, valvonnan tai oikeusturvan takia.

Köyhimpien maiden yksityisyyden ja tietosuojan puutteista on helppo hyötyä. Perinteisesti etenkin Yhdysvalloissa henkilötietojen suojan on katsottu suojaavan yksilöä nimenomaan valtiota vastaan,[84] mutta nykyisin suojaa tarvitaan myös horisontaalisesti eli yksityisten toimijoiden välillä. Esimerkiksi Facebook tarjoaa paikallisten operaattoreiden kautta rajoitettua mutta ilmaista verkkoa kehitysmaihin, minkä ansiosta Facebook voi seurata ja kontrolloida verkkoa käyttävien tietoja.[85] Internetiin pääsy ”maksetaan” Facebookille annettavilla tiedoilla käyttäjästä ja käyttäytymisestä internetissä, joten ilmainen verkko ei ole. Esimerkiksi Intia kielsi kyseisen verkon, mutta samalla monet menettivät pääsyn internetiin, mikä vaikeuttaa heidän elämäänsä. Rikkaammissa länsimaissa ihmisten ei tarvitse valita, antavatko tietojaan päästäkseen internetiin, vaan verkkoyhteys on itsestäänselvyys. Toki Facebook, Google ja monet muut toimijat keräävät tietoa länsimaissakin ihmisistä, mikä on uhka yksityisyydelle ja henkilötietojen suojalle, mutta sitä on mahdollista yrittää estää ilman, että menettää pääsynsä internetiin.

Kehittyneissä teollisuusmaissa demokratia yleensä toteutuu paremmin ja sen asema on turvatumpi kuin köyhemmissä, kehittyvissä maissa. Henkilötietojen suojan ja yksityisyyden puute mahdollistaa kansalaisten tarkkailun ja valvonnan, mistä seuraa, etteivät ihmiset välttämättä uskalla tuoda ajatuksiaan julki. Tämä mahdollistaa valtaapitävien oman aseman pönkittämisen, sillä toteutuakseen demokratia vaatii tilaa vapaalle ajattelulle, toiminnalle ja keskustelulle. Näin ollen köyhempien maiden asukkaiden on vielä vaikeampaa vaatia itselleen yksityisyyttä ja henkilötietojen suojaa. Vaikka kulttuurilla on vaikutusta yksityisyydelle annettavaan merkitykseen, teknologian tuoma parempi kontrollointimahdollisuus vaikuttaa myös suojan puutteeseen.

Lisäksi erittäin heikossa asemassa olevilla ihmisillä heidän yksityisyytensä, henkilötietojensa käyttö ja niiden suojaaminen eivät ole päällimmäisenä mielessä. Se ei tarkoita, että

[84] Blume 2002, s. 14.
[85] Ks. https://www.theguardian.com/technology/2017/jul/27/facebook-free-basics-developing-markets

yksityisyys kuuluisi vain rikkaille, mutta heikommassa asemassa olevien on vaikeampi vaatia sitä, kuten myös muita ihmisoikeuksia. Yksityisyys tai henkilötietojen suoja eivät ole heille tärkeimmässä päässä, mikäli esimerkiksi oikeus elämään tai oikeus vapauteen ovat vaarassa, vaikka yksityisyydensuoja voisi parantaa näidenkin toteutumista. Universaalisti hyväksyttyinä ihmisoikeuksina oikeus yksityisyyteen ja henkilötietojen suojaan kuuluu kaikille. Oikeuksien toteutuminen kuitenkin vain on heikompaa köyhempien ihmisten kohdalla, kun mahdollisuudet vaikuttaa ja vaatia oikeuksia ovat huomattavasti rajatummat.

3.2. Yksityisyyden ja henkilötietojen suojan suhde muihin oikeuksiin

3.2.1. Absoluuttisuus

Individualismi on kasvattanut alaansa länsimaissa, ja yksityisyys ja henkilötietojen suoja ovat vahvasti sidoksissa siihen. Jos ihminen nähtäisiin ainoastaan yhteisönsä jäsenenä eikä yksilönä, yksityisyydelle ei olisi tarvetta tai tilaa.[86] Mitä suurempi merkitys yksilöllä on, sitä vahvempaa suojaa annetaan yksityisyydelle ja henkilötietojen suojalle. Mikään oikeus ei kuitenkaan voi olla absoluuttinen — edes oikeutta elämään ei välttämättä voida pitää sellaisena.[87] Niinpä vielä vähemmän absoluuttisia ovat oikeus yksityisyyteen tai henkilötietojen suojaan. Kuitenkaan absoluuttisuuden puute ei vähennä niiden painoarvoa. Onkin sanottu, että tietyllä tapaa kaikilla muilla ihmisoikeuksilla on ulottuvuus oikeuden yksityisyyteen kanssa.[88]

Henkilötietojen suoja ja oikeus yksityisyyteen eivät voi olla absoluuttisia johtuen ensinnäkin suoraan käytännön seikoista. Individualismista huolimatta yksilö on aina osa yhteiskuntaa, jolloin hänen on käytännössä mahdotonta saavuttaa ”täydellistä” yksityisyyttä.[89] Yksilö ei voi itsenäisesti määrittää, mikä on hänelle yksityistä, vaikka hän kokisi tietyn asian hyvin henkilökohtaiseksi, sillä oikeuden ja laissa säädettyjen normien tulee yhdenvertaisuuden nimissä olla kaikille samat. On hieman huvittavaa, että juuri individualismia korostavalle oikeudelle olisi löydettävä kaikkia yhtäläisesti koskevat säännöt ja normit, jotta se olisi toimiva. Samoin henkilötietoja tarvitaan monissa eri yhteiskunnan toiminnoissa ja niiden käsittely on usein välttämätöntä. Täydellinen anonyymiys ei ole mahdollista, ja tietosuojanormien tarkoituksena ei olekaan kieltää henkilötietojen käsittelyä, vaan antaa

[86] Blume 2002, s. 9–10.
[87] Himma 2007, s. 862–863.
[88] Volio 1981, s. 193.
[89] Blume 2002, s. 16.

pelisäännöt, milloin käsittely on asianmukaista ja hyväksyttävää. Yksilö ei voi mitenkään täysin estää henkilötietojensa käsittelyä, mikäli hän haluaa olla osana yhteiskuntaa. Toisaalta pitäisi myös pystyä sanomaan, mitä täydellinen henkilötietojen suoja tarkoittaa: anonyymiyttä vai vain esimerkiksi sitä, että henkilötiedot ovat aina suojassa tahoilta, joiden ei pitäisi päästä niihin käsiksi?

Toisekseen oikeuden absoluuttinen toteuttaminen vaatisi, että oikeus olisi selkeästi määriteltävissä, sillä ilman tyhjentävää määrittelyä ei oikeuden täysimääräistä toteutumista voida todeta. Kuten edellä ilmeni, määrittely ei onnistu yksityisyyden kohdalla. Vaikka henkilötiedoissa käsitteenmäärittely on mahdollista ja se onkin tehty, ei henkilötiedoillekaan voida taata absoluuttista suojaa johtuen edellä puhutusta kiinteästä yhteydestä yksityisyyteen. Henkilötietojen suojalla pyritään turvaamaan myös yksityisyyttä, joten yksityisyyden ollessa määrittelyjen ulottumattomissa on mahdotonta arvioida, milloin henkilötietojen suoja on saavuttanut tämän tavoitteensa.

Absoluuttisuuden puute ilmenee myös normeista suoraan. Oikeuden yksityisyyteen takaavissa normeissa puhe on joko yksityisyyden kunnioittamisesta tai mielivaltaisen puuttumisen kieltämisestä. Lähtökohtaisesti kunnioittaminen osoittaa, että sen kohdetta pidetään arvossa, mutta mahdollistaa siitä poikkeamisen. Ilmaus on hankala, sillä kunnioittamisen määrää ja astetta on vaikea mitata. Vaikka yksityisyyttä kunnioitettaisiin vähemmän, sitä silti kunnioitetaan, joten kunnioituksen taso voi laskea salakavalasti. Niinpä raja on häilyvä, missä on menty liian pitkälle ja voidaan sanoa, ettei vaadittua kunnioitusta enää ole. Samoin henkilötietojen suojan kohdalla normeista ilmenee poikkeussääntöjä, joiden perusteella täydellinen henkilötietojen suojan toteutuminen jää haaveeksi. Tietosuoja-asetuksen johdannossakin sanotaan suoraan, ettei oikeus henkilötietojen suojaan ole absoluuttinen: sen on oltava oikeassa suhteessa muiden perusoikeuksien kanssa suhteellisuusperiaatteen mukaisesti, ja henkilötietojen suojan toteutumisessa on huomioitava sen yhteiskunnallinen tehtävä.[90] Myös EUT on oikeuskäytännössään todennut absoluuttisuuden puutteen,[91] eikä oikeuksien täysimääräiseen toteuttamiseen edes pyritäkään. Nimenomaan poikkeukset osoittavat merkittävän syyn, miksi absoluuttisuus ei milloinkaan toteudu. Toiset perusoikeudet ja intressit nimittäin toimivat yksityisyyttä ja henkilötietojen suojaa vastaan.

[90] TSA johdanto, kohta 4.
[91] Esim. C-92/09, kohdat 48 ja 50.

Selkeimmin yksityisyyttä ja henkilötietojen suojaa vastaan on sanavapaus, jonka käyttäminen saattaa loukata yksityisyyttä tai henkilötietojen suojaa. Jos kyse kuitenkin on asiasta, josta ihmisten tulisi saada tietää, oikeuden yksityisyyteen ei pitäisi voida estää sananvapauden toteutumista. Tapauskohtaisesti punnitaan, missä raja näiden välillä menee. Toisaalta yksityisyyden ja sananvapauden ja muiden demokraattisten oikeuksien voidaan katsoa kulkevan käsi kädessä. Vain silloin kun ihmiselle on turvattu oma yksityisyys, voi hän itsenäisesti ja toisista riippumatta muodostaa mielipiteensä ja osallistua demokraattisen yhteiskunnan toimintaan ja keskusteluun.[92] Hänen ei tarvitse pelätä omia ajatuksiaan ja niiden julkituomista kuten George Orwellin kirjoittamassa romaanissa Vuonna 1984. Ilman yksityisyyttä totalitarismi kukkii,[93] samoin kuin ilman sananvapauttakin.

Toinen selkeä syy rajoittaa yksityisyyden ja henkilötietojen suojan täydellistä absoluuttista toteutumista on turvallisuus. Yksityisyys luo piirin, johon siihen kutsumattomilla ei ole pääsyä, mikä samalla mahdollistaa kyseenalaisten toimien salaamisen. Turvallisuuden takaamiseksi ja vaaran ehkäisemiseksi näistä halutaan luonnollisesti tieto, mikä samalla tarkoittaa, että yksityisyyden piiriin on tunkeuduttava. Henkilötietojen avulla saadaan paljon tietoa ihmisten toiminnasta ja yhteydenpidosta, joten turvallisuuden nimissä myös henkilötietojen suoja saattaa joutua väistymään.

3.2.2. Yksityisyys ja henkilötietojen suoja vs. sananvapaus ja turvallisuus

YK:n vuonna 1993 järjestämässä ihmisoikeuskonferenssissa hyväksytyn Wienin julistuksen mukaan ihmisoikeudet ovat samanarvoisia keskenään ja niille on annettava sama painoarvo.[94] Lisäksi EIT on oikeuskäytännössään todennut oikeuden yksityisyyteen ja sananvapauden olevan samanarvoisia.[95] POK 52(3) art. mukaan EIS:ssa turvattuja oikeuksia vastaaville perusoikeuskirjan oikeuksille on annettava sama merkitys ja ulottuvuus kuin EIS:ssa, joten EIT:n oikeuskäytäntö on relevanttia myös EUT:lle.

Kun yksityisyys ja henkilötietojen suoja ovat vastakkain sananvapauden kanssa, täytyy niitä punnita toisiaan vastaan ja löytää ratkaisu, jossa sekä sananvapaus että yksityisyys ja henkilötietojen suoja toteutuisivat mahdollisimman hyvin antaen samalla sijaa toisillensa ja mahdollisille vastakkaisille intresseilleen. Sananvapauden ja henkilötietojen suojan välises-

[92] Blume 2002, s. 23.
[93] Forde 2016, s. 136.
[94] Wienin julistuksen kohta 5.
[95] Axel Springer AG v. Saksa, kohta 87.

tä välttämättömästä jännitteestä huolimatta niiden ei tarvitse sulkea toisiaan pois.[96] Itse asiassa EUT on todennut aikaisemmasta henkilötietodirektiivistä, etteivät sen säännökset *per se* sisällä sananvapautta koskevan yleisen periaatteen tai muiden, erityisesti EIS 10 artiklaa vastaavien oikeuksien ja vapauksien vastaisia rajoituksia.[97]

Esimerkiksi journalistien sananvapaus on normaalia laajempi johtuen heille kuuluvasta tehtävästä[98] kuten yleisön tiedottamisesta, demokraattisen keskustelun ylläpitämisestä ja vallan vahtikoirana toimimisesta. On myös huomattava, että sananvapaus käsittää oikeuden saada tietoa.[99] Sananvapaus ja journalismi on huomioitu TSA 85 artiklassa, jonka mukaan jäsenvaltioiden on säädettävä vapautuksia tai poikkeuksia henkilötietojen käsittelylle journalistisia tarkoituksia varten tai akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten. Tällöin edellytyksenä on, että poikkeus on tarpeen sananvapauden ja tiedonvälityksen vapauden yhteensovittamiseksi henkilötietojen suojan kanssa.

Journalismin käsitettä on EUT:n mukaan tulkittava laajasti, mutta poikkeus tulee kyseeseen vain, kun henkilötietoja käsitellään ainoastaan journalistisiin tarkoituksiin. EUT:n mukaan tämä tarkoittaa, että toiminnan ”ainoana tarkoituksena on tietojen, mielipiteiden tai ajatusten ilmaiseminen yleisölle”.[100] Laajakaan tulkinta ei siten kata esimerkiksi internetin hakukoneiden toimintaa. Se perustuu suoraan algoritmeihin, minkä takia journalistisen sisällön näkymistä hakutuloksissa voidaan pitää satunnaisena eikä varsinaisena journalismina.[101] Hakukone voidaankin velvoittaa poistamaan hakutuloksistaan linkkejä, vaikka tiedot säilyisivät lähdesivulla, joka mahdollisesti puolestaan kuuluu poikkeuksen piiriin.[102] Niinpä syntyy hieman ristiriitainen tilanne, sillä hakukoneiden jääminen TSA 85 artiklan ulkopuolelle käytännössä rajoittaa journalistisen, akateemisen, taiteellisen tai kirjallisen sisällön saamista, mitä poikkeussäännöillä on nimenomaan pyritty suojaamaan. Huomionarvoista on, että hakukoneet ovat nyky-yhteiskunnassa tiedonvälittäjinä hyvin tärkeitä, ja niillä on tunnustettu olevan erityisasema tietoyhteiskunnan kehityksessä.[103]

[96] Kuner 2012, s. 84.
[97] C-101/01, kohta 90.
[98] Pekkanen 1997, s. 19.
[99] Hijmans 2016, s. 230.
[100] C-73/07 (Satamedia ja Markkinapörssi), kohdat 56 ja 62. Tapauksessa sovellettiin HTD:ä, jonka 9 artikla vastaa nykyistä TSA 85 artiklaa.
[101] Ks. esim. EWHC 799, kohdat 98 ja 100.
[102] C-131/12, kohdat 82–86.
[103] Julkisasiamiehen ratkaisuehdotus C-131/12, kohta 36.

POK 52(3) artikla huomioiden EUT on omassa oikeuskäytännössään välttänyt ristiriitoja EIT:n kanssa.[104] Tästä huolimatta EUT:lla on ollut hyvin suoraviivainen ote yksityisyyden ja henkilötietojen suojan suhteesta sananvapauteen ja tiedonsaantioikeuteen. EUT:n mukaan oikeus yksityisyyteen ja henkilötietojen suoja lähtökohtaisesti ohittavat internetin käyttäjien intressin saada tietoa.[105] Näkökantaa on kritisoitu paljonkin, sillä se ohitti EIT:n yksityiskohtaisen oikeuskäytännön sananvapauden ja yksityisyyden välisestä punninnasta.[106] EUT:n näkemys on ollut ilmeisen vaikea hyväksyä, sillä esimerkiksi Englannin ja Walesin korkein oikeus katsoi EUT:n linjan olevan yhtenevä EIT:n oikeuskäytännön kanssa ja perusoikeuksien olevan siten samanarvoisia.[107] Näin ei EUT:n antaman ratkaisun mukaan ole, vaan kanta yksityisyyden ja henkilötietojen suojan etusijasta on päätöksessä hyvin selkeästi ilmaistu.

Vaikka EUT:n lähtökohtana ei ollutkaan sananvapauden ja oikeuden saada tietoa samanarvoisuus henkilötietojen suojan ja oikeuden yksityisyyteen kanssa, vastakkaisten oikeuksien punninta ei jäänyt huomiotta. Kyseessä olevien oikeuksien välisessä punninnassa tulee huomioida tietojen luonne ja niiden suhde rekisteröidyn yksityiselämään.[108] Niinpä henkilötietojen suojaa suhteessa sananvapauteen arvioidaan yksityisyyden linssin läpi. Samaten kussakin tilanteessa tulee huomioida yleisön intressi saada kyseiset tiedot. Tämän perusteella julkiselämässä aseman omaavan henkilön suoja on rajoitetumpaa, koska tällöin sananvapaus ja yleisön oikeus saada tietoa painavat poikkeuksellisesti henkilötietojen suojaa enemmän.[109]

Edellä mainitun linjauksen perusteella aseman julkiselämässä omaavilla henkilöillä on rajoitetumpi oikeus yksityisyyteen ja henkilötietojen suojaan, sillä heidän roolinsa takia yleisöllä on vahvempi ja perustellumpi oikeus saada tietoa kuin täysin yksityishenkilöiden kohdalla. EIT:n mukaan yleisöllä on perusteltu tiedonsaantioikeus julkisessa asemassa tapahtuvaan toimintaan, ja etenkin poliitikkojen yksityisyyden suoja on rajoitetumpaa yleisön intressin ja tiedonsaantioikeuden ulottuessa heidän kohdallaan tavanomaista pidemmälle.

[104] Rosas 2011, s. 204.
[105] C-131/12, kohdat 81 ja 99.
[106] Kulk – Zuiderveen Borgesius 2014, s. 392.
[107] EWHC 799, kohdat 132–134, viitatessa henkilötietojen suojan etusijaan todetaan ”the ’general rule’ – – was a descriptive, not a prescriptive one”.
[108] C-131/12, kohta 81.
[109] Ibid.

Mikäli julkaistut tiedot eivät mitenkään liity julkiseen asemaan vaan ovat täysin henkilökohtaisia, sananvapautta ja oikeutta saada tietoa tulee tulkita suppeammin.[110] Tällöin yleisön tiedonsaantioikeudelle ei ole legitiimiä perustetta, joten yksilön tulee saada suojaa yleisön intressin ohi, jolloin myös julkisessa asemassa olevilla on samankaltainen oikeus yksityisyyteen kuin tavallisilla yksityishenkilöillä. Ratkaisevaa intressin arvioinnissa EIT:n mukaan on, synnyttävätkö julkaistut tiedot demokraattista keskustelua ja ovat siten yhteiskunnallisesti relevantteja vai onko kyse vain ihmisten uteliaisuuden tyydyttämisestä lähinnä viihteen vuoksi.[111]

Yleisöllä on henkilötietojen ja yksityisyyden suojaa vahvempi tiedonsaantioikeus lähtökohtaisesti silloin, kun tiedon kautta yleisö saisi suojaa sopimattomalta menettelyltä, joten rajoitus koskee esimerkiksi poliitikkoja, liikemiehiä ja julkisessa virassa toimivia henkilöitä.[112] Asema julkiselämässä tarkoittaa eri asiaa kuin julkisuuden henkilö, sillä julkisessa asemassa voi toimia olematta varsinaisesti ihmisten yleisesti tunnistama julkisuuden henkilö. Julkisuuden henkilöllä, jolla ei puolestaan ole mitään todellista asemaa julkiselämässä, tulisi lähtökohtaisesti olla edellä esitetyn mukaisesti samankaltainen oikeus yksityisyyteen ja henkilötietojen suojaan kuin muillakin yksityishenkilöillä. Hyvin useat julkisuuden henkilöt kuitenkin kertovat itseään koskevia, mahdollisesti hyvin yksityisiä tietoja julkisesti. Mitä enemmän julkisuuteen annetaan tietoja itsestä, sitä kapeammaksi omaa yksityisyyttä rajataan sekä sitä myötä myös henkilötietoihin pääsyä. Jopa henkilötietojen, joiden käsittely on lähtökohtaisesti kiellettyä — esimerkiksi terveystietojen tai tietojen koskien yksilön etnistä alkuperää, uskonnollista vakaumusta tai poliittista mielipidettä — käsittely on sallittua, kun henkilö itse nimenomaisesti on saattanut tiedot julkisiksi (TSA 9(2) e kohta). Edes suostumusta ei tarvita, kun tiedot ovat jo julkisia. Yksityisyytensä ja henkilötietonsa voi siten menettää vain kerran.

Mutta tarkoittaako kerran julkiseen tehtävään tai virkaan ryhtyminen lopullista luopumista yksityishenkilönä olemisesta vai palautuuko henkilön yksityisyys entiselleen hänen julkisen asemansa päätyttyä? Esimerkiksi poliitikon lopettaessa poliittisen toimintansa ja ryhty-

[110] von Hannover v. Saksa, kohdat 63–66.
[111] von Hannover v. Saksa, kohta 76. Tapauksessa Monacon ruhtinaan Rainier III:n tytär, Hannoverin prinssin vaimo Caroline nosti kanteen Saksaa vastaan, joka oli sallinut lehdissä kuvien julkaisemisen hänen yksityiselämästään. Vaikka kyseessä on kiistatta julkisuuden henkilö ja Monacon hallitsijaperheen perheenjäsen, EIT katsoi hänen olevan yksityishenkilö ja hänen yksityisyyttään loukatun, sillä hänelle ei kuulunut mitään julkisia toimia. ks. myös Campmany y Diez de Revenga ja Lopez-Galiacho Perona v. Espanja sekä Bou Gibert ja el Hogar y la Moda S.A. v. Espanja.
[112] WP 225, s. 13.

essä vaikkapa yksityisyrittäjäksi hänen asemansa julkiselämässä lakkaa. Julkiseen asemaan liittyvät tiedot ovat tällöin edelleen yleisön saatavilla, mutta yksityiset tiedot, jotka henkilön aseman vuoksi olisivat aiemmin kuuluneet yleisön tietoon, eivät enää muille kuulu. Tietysti on käytännössä eri asia, kuinka irtautuminen onnistuu, jos asema julkiselämässä on myös tosiasiallisesti ollut julkinen siinä mielessä, että samalla on päätynyt julkisuuden henkilöksi.

Sanan- ja tiedonvälityksen vapauden lisäksi yksityisyyttä ja henkilötietojen suojaa vastaan vaikuttaa turvallisuus. Tilanteessa, jossa yksityisyys ja turvallisuus ovat vastakkain, turvallisuus yleensä voittaa.[113] Turvallisuutta pidetään siten tärkeämpänä, ja sen etusija yksityisyyteen ja henkilötietojen suojan suhteen on ilmennyt esimerkiksi Yhdysvaltojen toiminnasta erittäin selkeästi. Useat yhdysvaltalaiset tiedustelupalvelut ovat tunkeutuneet ihmisten henkilötietoihin ja yksityisiin asioihin pyrkiessään turvaamaan kansallisen turvallisuuden ja estääkseen mahdollisen terrorismin. Myös tietosuoja-asetuksessa on huomioitu turvallisuus. TSA 23 artiklan mukaan rekisteröidyn oikeuksia voidaan rajoittaa, jotta voidaan taata muun muassa kansallinen ja yleinen turvallisuus, puolustus ja rikosten ehkäiseminen. Sinänsä periaate on EU:ssa sama kuin Yhdysvalloissa, että henkilötietojen suoja väistyy sivummalle turvallisuuden toteutumiseksi. Käytännössä turvallisuuden ja henkilötietojen suojan ja yksityisyyden välisessä punninnassa syntyy kuitenkin hyvin suuria eroja riippuen siitä, minkälainen painoarvo kullekin annetaan.

[113] Himma 2007, s. 872–873.

4. EU:n mekanismit vaikuttaa globaalisti

Edellä on käsitelty yleisemmin yksityisyyttä ja henkilötietojen suojaa sekä niiden perus- ja ihmisoikeusasemaa. Seuraavissa luvuissa tutkimus keskittyy tarkemmin henkilötietojen suojaan EU:ssa ja siitä säädettyjen normien vaikutukseen EU:n ulkopuolella. Tässä luvussa tarkastellaan ensin, miksi henkilötietojen suojasta ylipäänsä on tarvetta säännellä ekstraterritoriaalisesti. Tämän jälkeen tutkitaan, kuinka EU pyrkii vaikuttamaan kansainvälisesti niin sanotusti perinteisellä tavalla. Tämä tarkoittaa esimerkiksi neuvotteluja kansainvälisistä sopimuksista ja ihmisoikeuksien edistämistä. Toinen tapa on vaikuttaa markkinatalouden ja EU:n oman taloudellisen voiman kautta niin kutsun Bryssel-efektin toteutuessa. Mekanismilla voidaan vaikuttaa toisiin valtioihin välinpitämättömämmin verrattuna perinteisiin neuvotteluihin ja kansainvälisiin sopimuksiin. Pehmein ja hienovaraisin tapa on vaikuttaa ihmisten käyttäytymiseen, jolloin valinnanvapaus edelleen säilyy heillä. Luvun lopussa tarkastellaan, minkälainen keino käyttäytymisen ohjaaminen on henkilötietojen suojassa.

4.1. Ihmisoikeuksien edistäminen

4.1.1. Henkilötietolainsäädännön ekstraterritoriaalisuuden tarve

Erityisesti Euroopassa oikeus yksityisyyteen ja henkilötietojen suoja ovat vahvasti nostettu ihmisoikeuksien joukkoon johtuen toisen maailmansodan ja Natsi-Saksan kauheuksien seurauksena syntyneestä pelosta henkilötietojen ja yksityisen tiedon väärinkäyttöön.[114] Oli oikeuden yksityisyyteen ja henkilötietojen suojan välisestä teoreettisesta suhteesta mitä mieltä tahansa, selvää on, että EU:ssa niiden asema on vahva. Molemmat oikeudet on kirjattu perusoikeuskirjaan ja suuntauksena on pyrkimys entistä parempaan suojaan, mitä uusi tietosuoja-asetus osoittaa. Rekisteröidyn katsotaan olevan huomattavasti heikommassa asemassa suhteessa rekisterinpitäjiin, minkä takia hyvin epätasapainoista suhdetta ja rekisteröityjen asemaa parantamaan on perustettu tietosuojaviranomaisia, joiden avulla rekisteröidyillä on myös enemmän valtaa kontrolloida tietojaan.[115] Aseman vahvuus ilmenee selkeästi myös edellä kerrotusta EUT:n tekemästä linjauksesta antaa yksityisyydelle ja henkilötietojen suojalle lähtökohtainen etusija yleisön tiedonsaantioikeutta vastaan.

Muualla asiat ovat toisin. Vaikka edellä yksityisyyden ja sitä kautta henkilötietojen suojan todettiin olevan universaalisti hyväksytty ihmisoikeus, erot eri maiden välillä ovat selkeitä.

[114] Stute 2015, s. 652, ja Svantesson 2014, s. 57.
[115] Gellert — Gutwirth 2013, s. 525.

Esimerkiksi Kiinassa on kehitteillä kasvontunnistusteknologiaan ja valvontakameroihin perustuva järjestelmä, joka seuraa kansalaisten käyttäytymistä ja jolla ihmisiä voidaan pisteyttää heidän luotettavuutensa mukaan ja vaikuttaa heidän toimintaansa.[116] Suhtautuminen henkilötietojen suojaan sekä yksityisyyteen tai valtion harjoittamaan seurantaan on Kiinassa siten hyvin erilaista kuin EU:ssa.

Vaikka Yhdysvaltojen ja Euroopan kulttuurit ovatkin suhteellisen lähellä toisiaan, ja lähtökohtaisesti näkemykset ihmisoikeuksista ovat melko samansuuntaisia, käsitykset yksityisyydestä ja henkilötietojen suojasta poikkeavat. Euroopassa niitä pidetään laajempina ja niiden katsotaan suojaavan yksilön ihmisarvoa sekä hänen mahdollisuuttaan ja oikeuttaa päättää julkisesta minästään. Yhdysvalloissa yksityisyyden ajatellaan olevan vapautta yksityisyyden piiriin tunkeutumisesta — etenkin valtion tekemästä tunkeutumisesta.[117] Kuten myöhemmin luvussa kuusi ilmenee, yksityisyyttä ja henkilötietojen suojaa ei ole Yhdysvalloissa arvostettu turvallisuuden mennessä niiden edelle, ja niiden asema on EU:hun verrattuna heikompi. Sääntely yksityisyydestä ja henkilötietojen suojasta on Yhdysvalloissa osittain puutteellista eikä lainkaan niin kattavaa kuin EU:ssa.[118]

Myös esimerkiksi Venäjän sääntely yksityisyydestä ja henkilötietojen suojasta poikkeaa EU:n linjasta perustellen sääntelyä kansallisella turvallisuudella. Uusi niin kutsuttu Yarovaya-laki velvoittaa internet- ja tietoliikenneyhtiöt säilyttämään käyttäjien tiedot, viestit, kuvat ja ääniviestit puolen vuoden ajan sekä viestinnän metatiedot kolmen vuoden ajan.[119] Tarkoitus on täydentää antiterrorismilainsäädäntöä, mutta uusi laki mahdollistaa Venäjän hallinnon kansalaisten entistä paremman vakoilun ja seurannan, mikä huomattavasti heikentää yksilöiden oikeutta yksityisyyteen ja henkilötietojen suojaan. Lainsäädäntö onkin kohdannut tiukkaa kritiikkiä.[120]

Edellä esitetyt esimerkiksi osoittavat, että EU:n ja kolmansien maiden välillä voi olla suuria eroja, kuinka henkilötietojen suojaan suhtaudutaan. Internet ja teknologia mahdollistavat henkilötietojen käsittelyn globaalisti, laajamittaisesti ja tehokkaasti niin, että EU:n alueella olevien ihmisten henkilötietoja voidaan käsitellä EU:n lainkäyttöpiirin ulkopuolella. EU:n on siksi ulotettava lainsäädäntönsä mahdollisimman laajalle turvatakseen alueellaan

[116] Ks. esim. http://www.bbc.com/news/world-asia-china-34592186 ja https://yle.fi/uutiset/3-10135093
[117] Whitman 2004, s. 1155–1159, 1161.
[118] Barclay 2013, s. 361.
[119] Lait 374-FZ ja 375-FZ, ks. Garrie – Byhovsky 2017, s. 247–248.
[120] Esim. Human Right Watch on kritisoinut uutta lainsäädäntöä, ks. https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights

olevien ihmisten henkilötietojen korkeatasoisen suojan. Muutoin kolmansien maiden heikompi henkilötietojen suoja aiheuttaa suojan alenemisen myös EU:ssa. Tätä ongelmaa voidaan yrittää paikata ekstraterritoriaalisella tietosuojalainsäädännöllä, joka vaikuttaisi myös kolmansissa maissa tapahtuvaan henkilötietojen käsittelyyn. EU:n tietosuojalainsäädäntö on globaalisti kaikkein vaikutusvaltaisinta ja se on suoraan vaikuttanut monien maiden omiin lakeihin henkilötietojen suojasta.[121] EU:n tietosuojanormeja vastaavien lakien säätäminen kolmansissa maissa ei kuitenkaan riitä suojaamaan EU:n tavoittelemaa henkilötietojen korkeatasoista suojaa, koska kaikki valtiot eivät näin kuitenkaan toimi tai mallia ottavat maat eivät välttämättä sääntele yhtä tiukasti kuin EU.

4.1.2. EU ihmisoikeuksien lähettiläänä

Oikeus yksityisyyteen ja henkilötietojen suoja ovat universaalisti hyväksyttyjä ihmisoikeuksia, vaikka täydelliseen yhteisymmärrykseen pääseminen ei kulttuurisista ja yhteiskunnallisista syistä johtuen olisikaan mahdollista. Jokaisen valtion tulisi turvata oikeuksien toteutuminen niiden kansainvälisten sopimusten mukaan, joihin se on sitoutunut. Ympäripyöreiden sanamuotojen ja puuttuvien valvonta- ja sanktiomekanismien takia oikeuksien toteutumisessa on eroja. Edellä esitettyjen esimerkkien valossa on myös selvää, että henkilötietojen suojaa ja oikeutta yksityisyyteen ei tosiasiallisesti edes pyritäkään suojaamaan kovin tehokkaasti ainakin eurooppalaisesta näkökulmasta katsottuna.

KP-sopimuksen 1 artiklan mukaan kaikilla kansoilla on itsemääräämisoikeus ja kaikkien sopimusvaltioiden tulee edistää tämän itsemääräämisoikeuden toteuttamista ja kunnioittaa sitä. Silti kansainvälisessä politiikassa mennään yleensä vahvimpien ehdoilla ja usein kansainvälisessä toiminnassa osapuolet pyrkivät edistämään omia intressejään ja etuaan. Myös EU on nimenomaisesti ilmaissut edistävänsä omia arvojaan ja eurooppalaisia intressejä.[122] Itse asiassa arvojen ja etujen edistäminen on yksi EU:n perussopimuksiin kirjatuista tavoitteista, sillä SEU 3(5) artiklan mukaan

> *”Unioni vaalii ja puolustaa arvojaan ja etujaan kansainvälisissä suhteissaan ja edistää osaltaan kansalaistensa suojelua. Se edistää osaltaan rauhaa, turvallisuutta, maapallon kestävää kehitystä, kansojen välistä yhteisvastuuta ja keskinäistä kunnioitusta, vapaata ja oikeudenmukaista kauppaa, köyhyyden poistamista ja ihmisoikeuksien, erityisesti lapsen oikeuksien suojelua, sekä*

[121] Bach – Newman 2007, s. 833, ja Svantesson 2014, s. 61.
[122] COM (2007) 581, s. 2 ja 5.

kansainvälisen oikeuden tarkkaa noudattamista ja kehittämistä, etenkin Yhdistyneiden Kansakuntien peruskirjan periaatteiden kunnioittamista."

Kyseistä artiklaa kutsutaan EU:n lähetysperiaatteeksi,[123] jonka lisäksi myös SEU 21 artiklan 1 kohta luo pohjaa EU:lle toimia kansainvälisissä yhteyksissä normatiivisesti. Sen mukaan

"*Unionin toiminta kansainvälisellä tasolla perustuu sen perustamisen, kehittämisen ja laajentumisen johtoajatuksena oleviin periaatteisiin, joita unioni pyrkii edistämään muualla maailmassa: demokratia, oikeusvaltio, ihmisoikeuksien ja perusvapauksien yleismaailmallisuus ja jakamattomuus, ihmisarvon kunnioittaminen, tasa-arvo ja yhteisvastuu sekä Yhdistyneiden Kansakuntien peruskirjan periaatteiden ja kansainvälisen oikeuden noudattaminen.*

Unioni pyrkii kehittämään suhteita ja rakentamaan kumppanuuksia sellaisten kolmansien maiden ja kansainvälisten, alueellisten tai maailmanlaajuisten, järjestöjen kanssa, jotka noudattavat ensimmäisessä alakohdassa mainittuja periaatteita. Se pyrkii edistämään yhteisten ongelmien monenvälistä ratkaisemista erityisesti Yhdistyneiden Kansakuntien puitteissa."

Saman artiklan toisessa kohdassa määritellään vielä tarkemmin EU:n tavoitteita kansainvälisissä suhteissa ja yhteistyössä kolmansien maiden kanssa. Perusteita EU:n halulle edistää ja viedä arvojansa yli omien rajojensa ei siten tarvitse etsiä kaukaa: pyrkiessään vaikuttamaan kolmansien maiden lainsäädäntöön ja toimintaan EU yksinkertaisesti toteuttaa sitä, mitä sen tehtäväksi ja päämääräksi on asetettu sen perustamissopimuksessa. EU:n lähtökohtana ei kuitenkaan ole taistelu muita vastaan. Esimerkiksi globalisaatiosta syntyvä kolmansien maiden ihmisten hyvinvoinnin kasvaminen ei ole uhka eikä tarkoita EU:n köyhtymistä, vaan yleinen hyvinvoinnin kasvu voi niin ikään kasvattaa myös eurooppalaisten hyvinvointia, kunhan toimitaan oikein.[124]

EU:n toimintaa pidetään usein imperialistisena,[125] mikä olisi vastoin kansojen itsemääräämisoikeutta. Vaikka EU pyrkii toimimaan kansainvälisissä yhteyksissä normatiivisesti, toimia ei voida kuitenkaan pitää ainakaan kulttuurisena imperialismina, sillä EU on usein

[123] Herlin-Karnell 2012, s. 1227–1230.
[124] KOM (2005) 525, s. 9.
[125] Zielonka 2008, s. 475.

riidoissa muiden kehittyneiden OECD-maiden kanssa.[126] Lisäksi ihmisoikeuksien kohdalla imperialismiväitteet ovat mielestäni perusteettomia. Väite ihmisoikeuksien perustumisesta länsimaisille arvoille on sinänsä ymmärrettävä, mutta ihmisten hyvinvoinnin kasvu ja yhteiskunnan kehittyminen ihmisoikeuksien edistämisen myötä on tosiasia. SEU 5 ja 21 artiklojen perusteella EU haluaa olla ihmisoikeuksien edistäjä ja rauhanrakentaja maailmassa, ei muita hallitseva imperiumi. Yleisen hyvän edistäminen ei ole imperialistista, varsinkin kun kepin sijaan käytetään porkkanaa. EU on ihmisoikeuksien edistäjänä huomattavasti suopeampi kuin Yhdysvallat eikä EU harjoita siinä suhteessa pakkoa kolmansia valtioita kohtaan. EU:n keinoina on tarjota lainsäädäntönsä implementointia vastaan esimerkiksi apua tai kaupankäynnin liberalisointia.[127]

EU:n vahvoista pyrkimyksistä huolimatta ihmisoikeuksien ja demokratian levittäminen ja vahvistaminen kolmansissa maissa on hyvin haastavaa, eikä EU ole onnistunut siinä.[128] EU on siten ollut lainkäyttönsä suhteen vain ”haukkuva” eikä ”pureva”.[129] Neuvottelut tai pyrkimys sitouttaa ihmisoikeussopimuksiin eivät yleensä ole kovin tehokkaita keinoja etenkin näkemysten ollessa vahvasti ristiriidassa, ellei vastapuolella ole jotakin intressiä muuttaa periaatteitansa ja toimiansa. Joissakin valtioissa ei välttämättä ole houkutusta antaa kansalaisilleen parempaa henkilötietojen suojaa ja yksityisyyttä, sillä niiden puute on tehokas keino kontrolloida ihmisiä. EU:n pitäisi pystyä tarjoamaan jotakin muuta tilalle, jotta oman asemansa turvaamiseen pyrkivät valtionjohtajat edes voisivat harkita ihmisoikeussopimusten ja EU:n edistämien arvojen mukaisten normien säätämistä. Tästä johtuen ja myös omalla alueellaan olevien ihmisten henkilötietojen suojaamiseksi EU:n tulee käyttää vahvempia keinoja kuin neuvotteluja tai vetoomusten esittämistä, jotta sen tavoite korkeatasoisesta henkilötietojen suojasta toteutuisi.

EU:lla täytyy sen tähden olla ekstraterritoriaalista tietosuojasääntelyä. Lähtökohtaisesti ekstraterritoriaalinen lainkäyttövalta ymmärretään jonkin valtion lainkäyttövallaksi toisen valtion alueella. Se voi kohdistua lainkäyttövaltaa harjoittavan valtion omiin kansalaisiin omien rajojensa ulkopuolella tai kaikkien muidenkin toisessa valtiossa olevien ihmisten toimintaan.[130] Toisen määritelmän mukaan ekstraterritoriaalinen lainkäyttövalta tarkoittaa valtion rajojen ulkopuolisen toimijan, yleensä toisen valtion, toimien kontrolloimista tai

[126] Manners 2002, s. 252–253.
[127] Zielonka 2008, s. 476 ja 480.
[128] Bradford 2012, s. 58.
[129] Ks. Svantesson 2014, s. 58–59.
[130] Senz – Charlesworth 2001, s. 72.

niihin suoraan vaikuttamista.[131] Tässä tutkimuksessa ekstraterritoriaalisuutta lähestytään hyvin laajasti: huomio on EU:n sääntelyn tosiasiallisessa vaikutuksessa riippumatta siitä, vaikuttaako EU suoraan tai välillisesti kolmansien maiden lainsäädäntöön tai onko vaikuttaminen edes EU:n tarkoitus.

Jos asioista voidaan säännellä ekstraterritoriaalisesti, niistä ei tarvitse neuvotella. EU:ta on vaadittu harjoittamaan ekstraterritoriaalista lainkäyttövaltaansa kohtuullisessa suhteessa ja hyväksyttävästi siten, että se suojelisi alueellaan olevien ihmisten perusoikeuksia mutta säilyttäisi samalla kolmansien maiden suvereeniuden.[132] Vaatimus on osittain mahdoton toteuttaa, koska internetistä johtuen tietosuojanormien tulisi ideaalitilanteessa olla globaalisti sovellettavissa, jotta tietosuojassa ei olisi aukkoja. EU:lla ei toisaalta myöskään ole kompetenssia ja mitään suoria keinoa pakottaa suvereeneja kolmansia maita noudattamaan EU:n tietosuojalainsäädäntöä tai muuttamaan lainsäädäntöä sitä vastaavaksi. Vaikka ekstraterritoriaalisia normeja säädettäisiin internetiä koskien, ongelmaksi tulisi sen päättäminen, kenen asettamia normeja on noudatettava. Internet myös hämärtää suvereeniuden rajoja erittäin tehokkaasti. Periaatteessa kaikki valtiot voisivat säätää normeja koskien internetiä ja toimintaa siellä heidän valtionsa ja kansalaistensa suhteen. Samalla niillä ei ole velvollisuutta noudattaa toisten valtioiden säännöksiä omalla alueellaan.

Tietosuoja-asetuksen alueellinen soveltamisala on silti säädetty ekstraterritoriaaliseksi. Lähtökohtaisesti ekstraterritoriaalisen soveltamisen onnistuminen herättää kysymyksiä, mutta EU:lla on käytössään hyvin tehokas ase vaikuttaa kolmansissa maissa — nimittäin sen suuri markkinavoima. Aiemmin vaikutusvallan välineenä on käytetty aseellista tai poliittista valtaa, mutta niiden sijaan EU käyttää taloudellista valtaansa, jolla se voi edistää omaa lainsäädäntöään kolmansissa maissa.[133] EU onkin sisällyttänyt myös ihmisoikeusehtoja omiin kahdenvälisiin kauppasopimuksiin kolmansien maiden kanssa, vaikka WTO:lla on tiukka linja suhteessa tuonnin rajoittamiseen mahdollisten vientivaltiossa tapahtuneiden ihmisoikeusloukkausten perusteella.[134] Multi- tai bilateraaliset sopimukset kolmansien maiden kanssa eivät kuitenkaan ole lainkaan välttämättömiä EU:n normien edistämiselle ekstraterritoriaalisesti. Markkinavoimansa turvin EU voi ulottaa lainsäädäntönsä vaikutuksia omien rajojensa ulkopuolelle myös ilman sopimuksia, jotka usein sisältävät vääjäämättä kompromisseja. Kun kolmansiin maihin vaikutetaan EU:n sisämarkkinoita koskevalla lain-

[131] Svantesson 2014, s. 60.
[132] Taylor 2017, s. 196.
[133] Zielonka 2008, s. 475.
[134] Bradford 2012, s. 29–30, 58, ja Zielonka 2008, s. 479.

säädännöllä, mitään neuvotteluja ei tarvita, sillä sääntely koskee vain EU:n jäsenvaltioita. Niinpä vaikutus voi EU:n kannalta olla tehokkaampaa tällä tavoin kuin sopimusten tai esimerkiksi poliittisen painostuksen kautta. Tällaista EU:n sisämarkkinoihin kohdistuvan sääntelyn ekstraterritoriaalista vaikutusta kutsutaan Bryssel-efektiksi.

4.2. Vaikuttaminen markkinatalouden kautta

4.2.1. Bryssel-efekti

Vaikka EU on lainsäädännön suurvalta, sen vaikutusvalta on suuresti riippuvainen siitä, onko vastapuolella uhkana joutua EU:n sisämarkkinoiden ulkopuolelle vai ei. Mikäli uhkaa ei ole, EU:n valtakin on huomattavasti vähäisempi.[135] Lisäksi EU:n vaikutusvallan suuruus on riippuvaista siitä, kuinka yhtenäisesti EU:n jäsenvaltiot toimivat tai kuinka suuri vastapuoli on itse.[136] Sen sijaan, että EU pyrkisi suoraan vaikuttamaan kolmansien maiden lainsäätäjiin, on tehokkaampaa vaikuttaa pienempiin toimijoihin, joilla on kuitenkin yhteiskunnassa paljon merkitystä eli yrityksiin. Kyse on tällöin Bryssel-efektistä *de facto*, mikä syntyy helpommin kuin Bryssel-efekti *de jure*. Se puolestaan tarkoittaa, että kolmannen maan lainsäätäjä implementoi EU:n sääntelyä EU:n sisämarkkinoilla toimivien yritysten lobbauksen seurauksena.[137]

Tätä kautta EU onkin onnistunut osoittamaan olevansa merkittävä globaali toimija. Esimerkiksi lentokoneiden päästöjä koskevassa tapauksessa C-366/10 EU:n alueelle tulevien tai lähtevien lentokoneiden lentoyhtiöt velvoitettiin maksamaan EU:n sääntelyn mukaisia päästömaksuja. Tuomiossa EUT katsoi, ettei ilmailutoiminnan päästökauppaa koskeva EU:n direktiivi 2008/101 riko kolmansien maiden suvereeniutta, sillä direktiivi tulee sovellettavaksi vain silloin, kun lentokone laskeutuu tai lähtee EU:n alueelta ja on siten EU:n lainkäyttövallan piirissä.[138] Vaikka direktiivi ei periaatteessa ulota vaikutustaan EU:n alueen ulkopuolelle, käytännössä se kuitenkin tekee niin. Päästömaksut lasketaan lennon koko matkalta, eikä vain EU:n alueella tapahtuneesta lennon osuudesta, joka saattaa olla vain murto-osa etenkin kaukolentojen kohdalla. Lentoyhtiöiden on suostuttava maksamaan EU:n sääntelyn mukaiset maksut, elleivät ne halua käyttää toista vaihtoehtoaan eli lopettaa lentojansa EU:n alueelle kokonaan.

[135] Young 2015, s. 1235 ja 1242.
[136] Ibid. s. 1243, 1245, ks. myös s. 1246 taulukko, josta ilmenee jäsenmaiden yhtenäisyyden parantaneen EU:n vaikutusvaltaa merityötä koskevassa yleissopimuksessa.
[137] Bradford 2012, s. 6.
[138] C-366/10, kohdat 117–118 ja 124.

EU:n toiminta arvojensa, intressiensä ja normiensa edistämisessä rajojensa ulkopuolella ei siten läheskään aina tarkoita suoria kansainvälisiä neuvotteluja, sopimuksia tai esimerkiksi talouspakotteiden käyttöä. Kuten tapaus C-366/10 osoittaa, EU:lla on kyky vaikuttaa globaalisti paljon hienovaraisemmalla tavalla. Tapauksessa kiistaa aiheuttanut direktiivi kohdistui sisämarkkinoihin ja jäsenvaltioihin, mutta samalla myös niihin, jotka haluavat toimia EU:n alueella. Haukkuva lainkäyttö muuttuukin huomaamatta purevaksi lainkäytöksi, vaikka periaatteessa kolmansista maista tulevilla toimijoilla on mahdollisuus olla hyväksymättä sitä. Se kuitenkin tarkoittaisi EU:n markkinoiden ulkopuolelle jäämistä, mikä voi olla taloudellisesti kannattamattomampaa kuin EU:n sääntelyn noudattaminen.

Tiettyjen edellytyksien on kuitenkin täytyttävä, jotta Bryssel-efekti toimisi *de facto*. Ensinnäkin vaaditaan tarpeeksi suuret markkinat, jotta niille pääsyllä tai ulkopuolelle joutumisella olisi merkitystä. Tämän lisäksi tarvitaan riittävän vahvaa lainsäädäntökapasiteettia, jonka yhtenä tärkeänä osana on mahdollinen vaara saada sanktioita, mikäli normeja ei noudata. Muuten väärintoimimisesta ei ole mitään uhkaa, eikä Bryssel-efektiä synny. Näiden lisäksi normien tulee olla tiukempia kuin muualla ja kohdistuttava niin, ettei sääntelyn kohde voi karata toiseen lainkäyttöpiiriin.[139] Tämän takia sääntely, joka kohdistuu kuluttajien suojaamiseen, on erityisen tehokasta Bryssel-efektin kannalta, sillä kuluttajat pysyvät paikallaan, eikä sääntelyä voida siten kiertää toisin kuin esimerkiksi pääoman kohdalla.[140]

Tiukempi sääntely on tärkeää, sillä yleensä kansainvälisesti toimivat yritykset yhtenäistävät toimintojansa vastaamaan riman korkeimmalle asettavaa sääntelyä. Yleensä yrityksellä on samat toiminta- ja tuotantotavat ympäri maailmaa, sillä se on usein taloudellisesti tehokkainta. Tätä kautta tiukempaa sääntelyä noudetaan kaikkialla kyseisen yrityksen toiminta-alueella. Edellytyksenä silti on toiminnan joko oikeudellinen, teknillinen tai taloudellinen jakamattomuus. Muutoin on vaarana, että yritykset säilyttävät eri toimintatavat eri maissa eikä Bryssel-efektiä synny, vaikka kaikki edellytykset siihen muuten olisivatkin.[141]

Bryssel-efektistä on kyse esimerkiksi seuraavassa tapauksessa: Kolmannessa maassa sijaitseva yritys valmistaa kosmetiikkaa ja se haluaisi tuoda tuotteitaan myös EU:n sisämarkkinoille myytäväksi. Tuotteissa on kuitenkin ainesosa, jonka käytön EU on kieltänyt kosmetiikassa suojellakseen kuluttajien turvallisuutta ja terveyttä. Jotta yritys voisi päästä EU:n markkinoille, sen on muutettava tuotettaan vastaamaan EU:n tiukempia kemikaalisäännök-

[139] Bradford 2012, s. 10–13, 15–16.
[140] Ibid. s. 16–17.
[141] Ibid. s. 15 ja 18.

siä. Tuotannon tehokkuuden kannalta yrityksen ei ole kuitenkaan kannattavaa ylläpitää kahta eri tuotantolinjaa, jossa toisessa tehtäisiin tuotetta EU:n markkinoille ja toisessa muille markkinoille, joissa sääntely on löysempää. Toimiakseen taloudellisesti tehokkaasti ja päästäkseen EU:n markkinoille yritys alkaa valmistaa tuotetta vain yhdessä tuotantolinjassa niin, että se vastaa EU:n lainsäädännön vaatimuksia. Kun kolmannen maan markkinoille tulevat tuotteet ovat samoja kuin EU:n markkinoille vietävät, EU:n sääntely kuluttajien turvallisuudesta ja terveydestä on *de facto* vaikuttamassa myös kolmansissa maissa. Tämän toteutuminen kuitenkin vaatii vielä sen, että yritys hyötyy EU:n markkinoille pääsystä enemmän kuin mitä sille on tuotannon muuttamisesta ja EU:n sääntelyyn sopeutumisesta aiheutunut kuluja.[142] Muutoin tuotannon ja toimintatapojen muuttaminen ei ole kannattavaa.

Bryssel-efekti on EU:lle miellyttävä ja suhteellisen helppo tapa vaikuttaa globaalisti, sillä EU:n normien ekstraterritoriaalisen vaikutuksen voidaan sanoa olevan vain sivutuote, joka syntyy ikään kuin vahingossa EU:n säännellessään omia sisämarkkinoitaan. Keino on tehokas toteutuessaan, sillä kolmansilla mailla ei luonnollisestikaan ole sananvaltaa siihen, minkälaista ja kuinka tiukkaa sääntelyä EU omalla alueellaan haluaa. Jos EU katsoo kuluttajien suojaamisen tarpeelliseksi tietyllä tavalla, kaikkien toimijoiden on noudatettava sääntelyä EU:n alueella. WTO on kieltänyt syrjivän tuonnin rajoitukset, mutta kolmansien maiden yritykset eivät voi vedota EU:n sääntelyn olevan syrjivää, koska se koskee myös jäsenvaltioihin sijoittautuneita yrityksiä. Lisäksi henkilötietojen kannalta tarkasteltaessa WTO on myös sallinut tuonnin rajoituksiin poikkeuksia tilanteissa, joissa suojellaan yksityisyyttä henkilötietojen käsittelyyn liittyen.[143]

4.2.2. Bryssel-efekti henkilötietojen suojassa yleisesti

Bryssel-efekti *de facto* toteutuu yritysten kautta niiden tehdessä päätöksiään tuotannostaan ja toimintatavoistaan talouden ja markkinoiden perusteella. Yleisesti ottaen Bryssel-efektin toimiminen ihmisoikeuksien edistämisessä ei onnistu tehokkaasti, sillä sisämarkkinoihin kohdistuvan sääntelyn kautta EU ei voi juuri vaikuttaa siihen, onko kolmannessa maassa esimerkiksi kidutusta tai orjuutta. Sen sijaan henkilötietojen suojan suhteen Bryssel-efekti voi olla EU:lle ja sen sääntelyn ekstraterritoriaalisuudelle erittäin toimiva, koska henkilötiedot ovat nykyään vahvasti osallisena yritysten toiminnassa, markkinoissa ja ylipäätään

[142] Bradford 2012, s. 12.
[143] Kuner 2013, s. 52, ja ks. myös GATS XIV art. c kohdan ii alakohta.

taloudessa. Henkilötiedoilla on suuri arvo esimerkiksi mainonnassa.[144] Tilanne on EU:lle otollinen. EU voi vaikuttaa markkinoiden ja Bryssel-efektin avulla kolmansien maiden henkilötietojen suojaan yritysten toiminnan kautta *de facto* tai jopa mahdollisesti tietosuojalainsäädäntöön *de jure*, jolloin myös henkilötietojen suojan perus- ja ihmisoikeusasema vahvistuu kolmansissa maissa. Samalla EU voi välttää ikuisen kiistelyn ihmisoikeuksien perimmäisestä arvopohjasta ja väitetystä imperialismista liittyen ihmisarvojen edistämiseen omien rajojen ulkopuolella. EU:n toimintaa pidetään legitiimimpänä asioissa, joissa kuluttajille halutaan antaa parempaa suojaa, kuin ihmisoikeuksien ja demokratian edistämisessä.[145] Vaatiessaan alueellaan oleville ihmisille korkeaa henkilötietojen suojaa EU periaatteessa keskittyy ainoastaan sen sisäisiin asioihin, mutta ulkopuolelta tulevien on yhtä lailla noudatettava näitä sääntöjä.

Toteutuuko Bryssel-efekti sitten henkilötietojen suojan kohdalla? EU:lla on kiistämättä tarpeeksi suuret markkinat houkutellakseen yrityksiä alueelleen. Ostovoimakorjatun bruttokansantuotteen perusteella EU oli maailman toiseksi suurin talous vuonna 2017 Kiinan jälkeen ja ennen Yhdysvaltoja.[146] Sen lainsäädäntökapasiteetti on myös erittäin vahva henkilötietojen suojan sääntelyssä.[147] Tämän osoittaa myös se, että EU:n tietosuojanormit toimivat esikuvana useissa kolmansissa maissa. Henkilötietojen suojan osalta EU:lla on myös auktoriteettia antaa sanktioita normeja vastaan toimineille. Suurin sanktio tietosuoja-asetuksen tiettyjen normien rikkomisesta on 20 000 000 euroa tai 4 % yrityksen vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta edeltävältä tilikaudelta (TSA 85(5) art.), joten mahdolliset sanktiot voivat olla erittäin suuria. EU:n henkilötietolainsäädäntö on myös tiukinta maailmassa,[148] joten lainsäädännön tiukkuusedellytys täyttyy myös. Lisäksi sääntely kohdistuu EU:n alueella oleviin henkilöihin, joten kohde pysyy hyvin stabiilisti paikallaan eikä karkaa toiseen oikeudenkäyttöpiiriin.

Tähän mennessä kaikki edellytykset Bryssel-efektin toteutumiseksi henkilötietojen suojan kohdalla ovat täyttyneet. Viimeiseksi esteeksi Bryssel-efektin toteutumiselle muodostuu se, kuinka yritykset lopulta toimivat. Tämä riippuu siitä, onko yritysten toiminta henkilötietojen suojan osalta jakamatonta siten, ettei erillisten prosessien ja toimintatapojen ylläpito ole taloudellisesti kannattavaa tai teknisesti edes mahdollista. Lähtökohtaisesti tekninen jaka-

[144] Svantesson 2014, s. 55.
[145] Bradford 2012, s. 66.
[146] https://www.cia.gov/library/publications/the-world-factbook/rankorder/2001rank.html#ch
[147] Bach – Newman 2007, s. 835.
[148] Svantesson 2014, s. 55.

mattomuus toteutuu henkilötietojen kohdalla, kun suuresta tietomassasta ei ole mahdollista erottaa EU:n alueella olevia yksilöitä kolmansissa maissa olevista.[149] Vaikka toiminnot olisikin mahdollista jakaa teknisesti, on erittäin epätodennäköistä, että yritykset edes haluaisivat tehdä kyseistä erottelua EU:sta ja muualta peräisin olevien henkilötietojen välillä ja ylläpitää niiden käsittelyä koskien erillisiä toimintamalleja. Se saattaa epäkäytännöllisyyden lisäksi aiheutua yritykselle täysin turhia kustannuksia. Bryssel-efektin toteutuminen henkilötietojen suojassa on siten hyvin todennäköistä. Varmaa se ei kuitenkaan ole. Seuraavassa luvussa käsiteltävässä oikeudessa tulla unohdetuksi Googlen on ollut mahdollista helposti ilman suuria kustannuksia toteuttaa oikeus koskemaan vain EU:n aluetta, minkä seurauksena on syntynyt kiistaa kyseisen oikeuden globaalista ulottuvuudesta ja EU:n kompetenssista määrätä internetistä maailmanlaajuisesti.

Tiukemmassa sääntelyssä uhkana on aina se, että EU:n alueella sijaitsevat yritykset joutuvat kilpailussa huonompaan asemaan tiukemmista vaatimuksista aiheutuvien kustannusten takia, mikäli kolmansista maista tulevat yritykset voivat välttää ne. Sen tähden on tärkeää, että tiukemmat normit ulotetaan koskemaan myös EU:n ulkopuolelta tulevia yrityksiä. Henkilötietojen suojan aseman vahvistaminen siten johtaa samalla EU:ssa sijaitsevien yritysten mahdolliseen kilpailuetuun. Ne ovat jo joutuneet sopeutumaan tiukempaan sääntelyyn, kun kolmansista maista tulevat yritykset vielä käyttävät resurssejaan siihen. Välttämättä kyse ei ehkä olekaan vain paremmasta henkilötietojen suojasta, jota EU haluaa alueellaan oleville ihmisille. Suhtautumisellaan tietosuojaan EU voi yrittää hakea myös kilpailullista etua, eikä vain parantaa henkilötietojen suojaa perusoikeutena.[150] Tällöin EU ei toimikaan jalona ihmisoikeuksien edistäjänä vaan käyttää taloudellista valtaansa Bryssel-efektin kautta saadakseen itselleen lisää taloudellista etua — tahallaan tai tahtomattaan.

EU voidaan nähdä globaalina tietosuojan vartijana ja ”yksityisyyspoliisina”. Vaihtoehtoisesti mahdollista ekstraterritoriaalista vaikutusta voidaan pitää vain sivutuotteena, johon ei tietoisesti ole pyritty, ja EU:n tietosuojanormeja vastaavien lakien lisääntyminen globaalisti on vain käytännön seurausta.[151] Eriävät mielipiteet EU:n roolista ovat väistämättömiä, sillä EU:n perimmäisiä motiiveja säännösten takaa on lähes mahdoton selvittää. EU:n itsensä sisällä on nimittäin vahvasti eri näkemyksiä siitä, mikä EU:n roolin tulisi kansainvä-

[149] https://www.wired.com/2008/04/eu-tells-search/ ja Bradford 2012, s. 18 ja 25.
[150] Svantesson 2014, s. 57.
[151] Ks. Lynskey 2015, s. 43.

lisesti olla ja kuinka sen pitäisi toimia globaalissa kentässä.[152] EU:n normit ovat kompromissien tulos, minkä seurauksena niiden taustalla vaikuttavat aina sekä pelkästään EU:n omiin asioihin keskittyvät motiivit että motiivit pyrkiä vaikuttamaan laajemmin EU:n ulkopuolella. Tämä on linjassa sen kanssa, että EU:n pyrkimyksenä on edistää henkilötietojen suojan toteutumista ihmisoikeutena niin EU:ssa kuin sen ulkopuolellakin samalla huomioiden myös taloudelliset seikat ja kilpailun. Omien etujen ajaminenhan on osaltaan myös EU:n tavoitteena SEU 3(5) artiklan mukaisesti.

4.3. Pehmeä vaikuttaminen käyttäytymistä ohjaamalla

4.3.1. Nudging — tuuppimista parempaan käyttäytymiseen

Kovimman tason vaikuttamisessa kohteena ovat toiset valtiot ja keinoina sitovat ihmisoikeussopimukset tai esimerkiksi kansainvälinen politiikka. EU:n mahdollinen vaikuttaminen tapahtuu tällöin korkealla tasolla niin, että vaikutuksen syntyessä se tulee ylhäältä valtiontasolta alaspäin kansalaisiin. Bryssel-efektin kautta tapahtuva epäsuorempi mutta todennäköisesti tehokkaampi vaikuttaminen kohdistuu sen sijaan yrityksiin, jolloin vaikutus yhteiskuntaan tulee markkinoiden muutoksesta. Bryssel-efektin kautta vaikuttaminen ei ole niin kovaa kuin ihmisoikeuksien kautta tapahtuva. Vaikka se perustuukin EU:n lainsäädäntöön, yrityksen vallassa on valita, noudattaako se EU:n lainsäädäntöä myös kolmansissa maissa vai ei. Näiden lisäksi on mahdollista vaikuttaa myös erittäin pehmeästi huomioimalla ihmisten käyttäytyminen ja vaikuttamalla heidän valintoihinsa.

Ihmisen päätöksenteko ja ajattelu voidaan jakaa kahteen eri järjestelmään, jossa ensimmäisessä päätökset tehdään intuitiivisesti, nopeasti ja automaattisesti. Toisessa järjestelmässä ajattelu on hitaampaa, ja valinnat tehdään tietoisesti ja harkiten.[153] Etenkin taloudellisissa teorioissa kuluttajien oletetaan noudattavan päätöksissään toista, vahvaan harkintaan ja rationaaliseen ajatteluun perustuvaa järjestelmää. Näin ei useinkaan silti ole, vaan käyttäytymistieteellisestä lähtökohdasta tarkasteltuna ihmisten tiedostetaan tekevän päätöksiä myös ensimmäisen, intuitiivisemman järjestelmän ohjaamina.[154] Tämä huomioimalla ihmisiin voidaan vaikuttaa hyvin pehmeästi ilman sääntelyäkin.

[152] Bradford 2012, s. 63.
[153] Kahneman 2011, s. 20–21.
[154] Codagnone et al. 2014, s. 52.

Vaikuttaminen ihmisten käyttäytymisen kautta tapahtuu muuttamalla valinta-arkkitehtuuria siten, että niin kutsutuilla ohjaimilla yksilöä ”tuupitaan” tekemään tietty, oikeampi ja parempi valinta kuitenkin säilyttämällä yksilön valinnanvapaus.[155] Käytännössä tämä tarkoittaa, että yksilölle tehdään helpommaksi ja houkuttelevammaksi toimia itsensä ja yhteiskunnan kannalta yleensä rationaalisemmin, terveellisemmin tai muuten paremmin. Esimerkiksi lisäämällä roskakorien näkyvyyttä roskaaminen vähentyy selvästi. Samoin asettamalla paremmat oletusasetukset yksilön pitää nähdä vaivaa vaihtaakseen asetusta toiseen, itselleen tai ympäristölle huonompaan vaihtoehtoon, jolloin paremmat päätökset lisääntyvät ihmisten usein ollessa passiivisia.[156] Varsinaisesti tällöin ei välttämättä ole edes tehty tietoista päätöstä, mutta yksilöllä on silti ollut mahdollisuus valita toisin, jos hän olisi halunnut. Ohjaimilla vaikuttaminen onnistuu, kun ”oikean” valinnan tekemisestä tehdään helppoa ja houkuttelevaa, ohjaaminen tapahtuu oikea-aikaisesti ja myös ympärillä olevat ihmiset toimivat samalla tavoin.[157]

Valinta-arkkitehtuurin muuttaminen ja käyttäytymisen ohjaaminen ei kuitenkaan automaattisesti tarkoita, että paremmat valinnat lisääntyisivät. Ihmisten päätöksenteko muuttuu siten kuin sitä ohjataan, niin parempaan kuin huonompaankin suuntaan. Tästä syystä käyttäytymiseen vaikuttamisessa on aina mukana vastuu siitä, miten ihmisten käyttäytymistä ohjataan. Usein käyttäytymiseen vaikuttaminen on huomaamatonta, ja ihmiset toimivat tiedostamattaan toisin. Esimerkiksi varoitusteksteillä voidaan vaikuttaa ihmisten internetkäyttäytymiseen siten, että heidän kyberturvallisuutensa parantuu. Käyttäytymisen muutoksesta huolimatta he eivät kuitenkaan kokeneet tietävänsä paremmin, kuinka suojautua verkkoympäristön uhilta.[158]

Vaikuttamista ihmisten käyttäytymiseen parempaan suuntaan pidetään paternalistisena. Kun ihmisillä silti säilytetään oma valinnanvapaus, kyse on libertaristisesta paternalismista.[159] Yksi suurimmista syistä vastustaa paternalismia on se, että yksilön tulee saada valita siitä huolimatta, että valinta menisi pahastikin pieleen.[160] Ihmiset eivät halua holhousyhteiskuntaa, koska se vähentää heidän valinnanmahdollisuuksiaan, ja tämä koetaan vapau-

[155] Sunstein 2014, s. 17, viittaus teokseen Thaler, Richard H. – Sunstein, Cass R.: Nudge. Improving Decisions about Health, Wealth and Happiness (2008), s. 8. Thaler ja Sunstein puhuvat termistä nudge, joka tarkoittaa suomeksi tönimistä tai tuuppimista.
[156] Ks. Halpern 2015, s. 94, 62–64.
[157] Halpern 2015, s. 60, 65, 83, 108 ja 128.
[158] van Bavel – Rodríguez-Priego 2016. s. 2–3.
[159] Thaler – Sunstein 2003, s. 175.
[160] Sunstein 2014 s. 21, 89.

den rajoittamisena. Henkilötietojen suojassa yksilön valinnanvapaus voi kuitenkin olla erittäin ongelmallista. Kuten edellä on tullut ilmi, yksityisyyden menettämiseen riittää vain yksi kerta, ja mikäli henkilötiedot päätyvät vääriin käsiin tai arkaluonteiset tiedot internetiin, niiden saattaminen takaisin suojaan on erittäin vaikeaa. Jos henkilö ei täysin ymmärrä omien tietojensa tärkeyttä ja hän tekee henkilötietojen suojan tai yksityisyyden kannalta huonon valinnan, hän voi ymmärtämättömyyttään mahdollistaa henkilötietojensa ja yksityisyytensä vakavankin loukkauksen. Tässä mielessä hieman holhoava vaikuttaminen on perusteltua.

4.3.2. Henkilötietojen suojaan liittyvään käyttäytymiseen vaikuttaminen

Käyttäytymiseen vaikuttaminen kohdistuu aivan ruohonjuuritasoon eli yksilön toimintaan, päätöksiin ja asenteisiin. Oman alueen asukkaiden käyttäytymisen ohjaaminen onnistuu helpommin, sillä he ovat paremmin paternalistisen ohjaajan vaikutuspiirissä. Jotta EU voisi vaikuttaa ihmisten käyttäytymiseen myös rajojensa ulkopuolella, sen täytyy ensin saada siellä olevat yksilöt vaikutuspiiriinsä. Tämä onnistuu esimerkiksi järjestämällä kansainvälisiä konferensseja tai koulutustilaisuuksia.[161] Tällöin käyttäytymiseen vaikuttaminen ei kuitenkaan tapahdu päätöksenteko- tai toimintahetkellä, kuten roskakorille ohjaamisessa. Sen sijaan tätä kautta voidaan vaikuttaa henkilötietojen suojaan suhtautumiseen ja asenneilmapiiriin. Vaikuttaminen voi siten olla hieman vaikeampaa mutta samalla myös pysyvämpää verrattuna esimerkiksi tilanteeseen, jossa käyttäytymisen ohjaaminen tapahtuu oletusasetuksia muuttamalla ja perustuu ihmisten passiivisuuteen.

Tiedon välittäminen ja eräänlainen valistus on käyttäytymiseen vaikuttamista yksinkertaisimmillaan.[162] Pelkkä tiedon antaminen ei välttämättä saa ihmisiä tekemään parempia päätöksiä, koska ihmisen toimintaan vaikuttaa tiedostamatta koko häntä ympäröivä konteksti.[163] Kun informaatio esitetään oikeassa muodossa eli helposti ymmärrettävästi ja selkeästi, sen vaikutus kasvaa huomattavasti.[164] Yksityisyyteen liittyvien päätösten aineellisia ja aineettomia seurauksia on kuitenkin usein erittäin vaikea arvioida, ja hienovaraiset painotukset ja tehosteet voivat helposti vaikuttaa tietosuojalle annettavaan merkitykseen ja siihen, kuinka tietosuojaan liittyen toimitaan.[165] Niinpä henkilötietojen suojassa vaikuttami-

[161] Ks. esim. Euroopan tietosuojavaltuutettu toimi kansainvälisen tietosuojakonferenssin isäntänä vuonna 2018 https://www.privacyconference2018.org/.
[162] Halpern 2015, s 183.
[163] Codagnone et al. 2014, s. 52.
[164] Halpern 2015, s. 184.
[165] Acquisti 2009, s. 83.

nen valistuksella voi olla hyvin vaikeaa, sillä etenkin verkkoympäristöön liittyvät uhat ja tietynlaisen toiminaan seuraukset eivät välttämättä selkeästä tiedottamisesta huolimatta konkretisoidu ihmisille tai ne on hankala ymmärtää. Tietosuojaa ja yksityisyyttä koskevaan käyttäytymiseen voidaan vaivattomammin vaikuttaa käyttämällä tiedottamisen lisäksi huomaamattomampia ohjaimia, kuten oletusasetusten säätämistä. EU:ssa olevien toimijoiden olisi mahdollista tällä tavoin ohjata käyttäytymistä myös rajojen ulkopuolella esimerkiksi internetpalveluissa, mutta sen toteutuminen on hyvin haastavaa todentaa.

Liiallisella valistuksella on lisäksi kääntöpuolensa. Uutiset tietomurroista, -vuodoista ja -uhkista sekä monimutkaiset yksityisyys- ja henkilötietoasetukset johtavat helposti ns. yksityisyysväsymykseen. Ihmiset kokevat, ettei heillä ole lainsäädännöstä huolimatta vaikutusvaltaa omien henkilötietojensa käyttöön ja he luovuttavat asian suhteen.[166] Lopputuloksena rekisteröidyt hyväksyvät kaiken henkilötietojen käytön ilman sen syvällisempää pohdintaa, sillä se on rekisteröidylle yksinkertaisin ja nopein tapa päästä eteenpäin.[167] Ihmisten liian tehokas tiedottaminen voi toimia itseään vastaan ja lisätä väsymystä entisestään.

Asiantuntijoihin tällä ei sen sijaan ole niinkään merkitystä heidän roolinsa takia. Siten kansainväliset tapahtumat ja konferenssit voivat vaikuttaa EU:n ulkopuolelta tuleviin positiivisella, parempaan tietosuojaan tähtäävällä tavalla, jolloin he mahdollisesti pyrkivät toimimaan kotimaissaan sen mukaisesti. Tietosuoja-ammattilaisille on myös tarjolla koulutuksia, jolla he voivat hankkia itselleen esimerkiksi sertifikaatin tietosuojaosaamisestaan.[168] Tämä ensinnäkin voi lisätä EU:n tietosuojalainsäädännön tuntemusta kolmansissa maissa, mutta toisekseen myös vaikuttaa asenteisiin ja käyttäytymiseen. Näin on etenkin silloin, kun käsitykset yksityisyydestä ja henkilötietojen suojasta ovat samansuuntaiset EU:n kanssa. Sen sijaan totalitaaristen maiden kohdalla on epäuskottavaa, että tämänkaltaista vaikutusta voisi yksilöiden kautta juurikaan syntyä, kun yksilön mahdollisuudet toimia toisin tai vaatia muutosta ovat hyvin rajatut.

Paternalistisen ohjauksen ei tarvitse tulla ylemmältä tasolta, vaan sitä voi tehdä kuka tahansa asian osaava toimija, esimerkiksi yritys. Erityisen tehokasta ohjaimilla vaikuttaminen on silloin, kun kuluttajia ohjataan ohjaamaan valmistajien ja yritysten toimintaa.[169] Tämä tarkoittaa, että kuluttajien käyttäytymiseen vaikutetaan niin, että he tekisivät parem-

[166] Choi et al. 2018, s. 42–43, “privacy fatigue”.
[167] Ibid. s. 44.
[168] Ks. esim. https://www.eipa.eu/dataprotection/.
[169] Halpern 2015, s. 170, “double nudge”.

man valinnan, mikä puolestaan lisää tai heikentää jonkun tuotteen tai palvelun kysyntää. Sen seurauksena yritykset reagoivat kuluttajien käyttäytymisen muutokseen ja tarjoavat heille kysyntää vastaavaa tuotetta tai palvelua. Käyttäytymisen ohjaaminen ei välttämättä kuitenkaan lopu tähän. Tarjonnan muuttuessa ja tuotteiden kehittyessä vaikutus leviää koskemaan myös niitä kuluttajia, jotka eivät alun perin olleet muuttaneet valintojaan tai jotka olivat olleet vähemmän valistuneita.[170] Tämä on tehokasta sen takia, että muutoksen aikaansaamiseen ei tarvita suurten massojen käyttäytymisen ohjaamista, vaan vähempikin riittää.[171]

Jos tarpeeksi moni kuluttaja muuttaa käyttäytymistään henkilötietojensa suojan suhteen vastaten EU:n tavoittelemaa parempaa suojaa, se voi mahdollisesti vaikuttaa yritysten toimintaan. Kansainvälisten yritysten kohdalla toimintamallit sekä tarjotut tuotteet ja palvelut leviävät kaikkialle, missä ne toimivat. EU:n näkemyksiä henkilötietojen suojasta voidaan levittää sen rajojen ulkopuolelle jälleen yritysten kautta samoin kuin Bryssel-efektissä, jos yritykset muuttavat tarjontaansa globaalisti ohjaten samalla kolmansissa maissa olevien ihmisten käyttäytymistä. Erona on, että Bryssel-efektissä toiminnan muutos on seurausta tosiasiallisesta pakosta, jos yritys haluaa toimia EU:n sisämarkkinoilla, mutta nudge-vaikuttamisessa muutos on vapaaehtoista. Yksityisyysväsymyksen uhallakin kuluttajien valituksella ja tiedottamisella on siten merkitystä, koska tietoisuus lisää kuluttajien vaatimuksia. Haasteena kuitenkin on aluksi vaikuttaa tarpeeksi monen kuluttajan käyttäytymiseen siitä huolimatta, että pienempikin määrä riittää saamaan laajan vaikutuksen. Mitä suurempi yritys on, sitä enemmän tarvitaan kuluttajia muuttamaan sen toimintaa ja tarjontaa. Mutta jos se onnistuu, voidaan suurten yritysten kautta vaikuttaa erittäin laajasti.

Kuten jo Bryssel-efektin kohdalla kävi ilmi, korkeatasoisesta henkilötietojen suojasta voidaan tehdä myös kilpailuvaltti. Tällöin toiset yritykset mahdollisesti vastaavat henkilötietojen suojaa painottavan yrityksen etusijaan parantamalla itsekin tietosuojaa — ehkä jopa EU:n asettamalle tasolle. Lisäksi jo pelkästään pakollisten tietosuojavaatimusten täyttämisestä voidaan hakea hyötyä. Esimerkiksi tietosuoja-asetuksen mukaiset, rajat ylittävissä tietojensiirroissa vaadittavat tietosuojasertifioinnit voivat myös olla luomassa nudge-vaikutusta, jos sertifioinneista esimerkiksi mainitaan markkinoinnissa. Kuluttajalle voi kolmannessakin maassa syntyä käsitys kyseisen yrityksen paremmasta toiminnasta, jonka perusteella hän ohjautuu valitsemaan tietosuojan kannalta paremmin toimivan yrityksen.

[170] Halpern 2015, s. 171, ”triple-nudge”.
[171] Ibid. s. 170.

5. Oikeus tulla unohdetuksi ja sen ekstraterritoriaalisuus

Seuraavassa keskitytään tarkemmin kahteen henkilötietojen suojaan kuuluvaan osa-alueeseen ja niitä koskevan lainsäädännön vaikutuksen ulottumiseen EU:n ulkopuolelle. Tässä luvussa tarkastelun kohteena on rekisteröidyn oikeus tulla unohdetuksi, joka on taattu sekä tietosuoja-asetuksessa että sitä edeltäneessä direktiivissä. Asioiden unohtaminen on ollut ihmiselle lähtökohta ja muistaminen vain poikkeus. Nykyisen teknologian seurauksena osat ovat vaihtuneet, ja muistamisesta on tullut pääsääntö unohtamisen muuttuessa yhä poikkeuksellisemmaksi.[172] Tämä voi johtaa yksilön kannalta kohtuuttomaan tilanteeseen, jota pyritään parantamaan oikeudella tulla unohdetuksi. Kyseinen oikeus on myös erinomainen esimerkki pyrkimyksistä antaa rekisteröidylle vahvempi kontrollivalta omiin henkilötietoihinsa, mikä on yksi tietosuoja-asetuksen lähtökohdista.[173]

Yksi merkittävimmistä oikeuteen tulla unohdetuksi liittyvistä EUT:n oikeustapauksista on ns. Google Spain -tapaus (C-131/12). Kyseinen oikeus ei syntynyt tapauksen myötä, vaikka niin usein saatetaan ajatella. Eurooppalaiset juuret oikeudelle tulla unohdetuksi löytyvät Ranskan oikeudesta. Rikoksesta tuomittu tietyssä mielessä armahdettiin antamalla hänelle oikeus vastustaa julkaisuja hänen tuomiostaan, kun annettu rangaistus oli suoritettu, eli hänelle suotiin oikeus tulla unohdetuksi.[174] Google Spain -tapauksessa oikeuden tulla unohdetuksi vahvistettiin ensi kertaa kohdistuvan myös internetin hakukoneisiin, mikä tekee siitä tärkeän ratkaisun.[175] Linjaus on merkittävä, koska suurin painoarvo oikeudella tulla unohdetuksi on julkisissa, kaikille avoimissa rekistereissä, ja internetin hakukoneet ovat juuri tällaisia rekistereitä. Niistä kuka tahansa voi saada paljonkin henkilöä koskevaa tietoa, jolloin intressi oikeudelle tulla unohdetuksi on suuri. Samalla EU:n tavoittelema henkilötietojen korkeatasoinen suoja on mahdollisesti uhattuna. Tämän luvun ensimmäisessä osassa käsitellään siten sitä, mistä oikeudessa tulla unohdetuksi on kyse etenkin internetin hakukoneiden kohdalla.

Koska internetissä julkaistut tiedot ja hakukoneiden tulokset ovat ihmisten saatavilla ympäri maailmaa, oikeuden tulla unohdetuksi toteutumisen kannalta on tärkeää tarkastella myös EU:n lainsäädännön alueellista soveltamisalaa sekä sen mahdollista vaikutusta kolmansissa maissa. Tätä käsitellään tämän luvun toisessa osassa. EU:n pyrkimys taata sen alueella

[172] Mayer-Schönberger 2009, s. 2.
[173] TSA johdanto kohta 7.
[174] Rosen 2012, https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/
[175] Taylor 2017, s. 197.

oleville henkilöille oikeus tulla unohdetuksi osana henkilötietojen suojaa jää pahasti puolitiehen, mikäli oikeus ei toteudu EU:n ulkopuolella. Hakukoneiden toiminta siellä vaikuttaa suoraan EU:n tietosuojalainsäädännön takaamien oikeuksien tosiasialliseen toteutumiseen. Ongelmina on, voidaanko EU:n tietosuojanormeja soveltaa EU:n ulkopuolella sijaitseviin hakukoneisiin ja täytyykö hakukoneen noudattaa EU:n sääntelyä muualla kuin EU:ssa vai voivatko poistetut tiedot olla edelleen näkyvillä kolmansissa maissa. Koska Google Spain -tapauksessa sovellettiin vielä aikaisempaa henkilötietodirektiiviä, seuraavassa puhutaan myös siitä tietosuoja-asetuksen ohella.

5.1. Google Spain ja korkeatasoinen henkilötietojen suoja

5.1.1. Hakukone rekisterinpitäjänä ja sen vastuun laajuus

Espanjalaisessa La Vanguardia -lehdessä oli vuonna 1998 ollut kahdesti ilmoitus kiinteän omaisuuden huutokaupasta liittyen Mario Costeja Gonzálezin sosiaaliturvasaatavien perimiseksi suoritettuun takavarikkoon. Tässä yhteydessä mainittiin Gonzálezin nimi. Koska internet ei unohda, samat ilmoitukset löytyivät Googlen hakutuloksista vielä 16 vuotta myöhemmin, kun haun teki Gonzálezin nimellä. González teki tämän johdosta kantelun La Vanguardia -lehdestä sekä Google Spainista ja Google Inc:sta AEPD:lle (Agencia Española de Protección de Datos, Espanjan tietosuojaviranomainen) vaatien, että kyseinen lehti poistaisi hänen nimensä sisältävät internetsivut tai piilottaisi hänen henkilötietonsa ilmoituksesta. Samoin hän vaati, että Google poistaisi tai ei enää näyttäisi linkkejä kyseisille La Vanguardian internetsivuille hänen nimellään tehdyissä hakutuloksissa.[176]

AEPD hylkäsi kanteen La Vanguardian osalta, sillä tiedot oli julkaistu työ- ja elinkeoministeriön määräyksestä ja se oli ollut perusteltua, jotta huutokauppaan olisi saatu mahdollisimman paljon osanottajia. Sen sijaan AEPD hyväksyi kantelun Google Spainin ja Google Inc:n (myöhemmin yhdistettynä Google) osalta. AEPD katsoi, että hakukone voidaan määrätä poistamaan tietoja, jos ne loukkaavat tietosuojaa ja ”henkilöiden arvokkuutta laajassa mielessä, mikä pitää sisällään myös rekisteröidyn pelkän tahdon siitä, etteivät sivulliset saa selville näitä tietoja”.[177] Tämän seurauksena Google nosti kanteen Audiencia Nationalessa, joka teki asiassa ennakkoratkaisupyynnön EUT:lle henkilötietodirektiivin soveltamisesta.

[176] C-131/12, kohdat 14–15.
[177] C-131/12, kohdat 16–17.

Ennakkoratkaisupyynnössä kysyttiin ensinnäkin tulkintaa direktiivin ja sen myötä kansallisen täytäntöönpanonormiston alueelliselle soveltamisalalle. Asiassa oli riidanalaista, voitiinko henkilötietoja käsittelevään, Yhdysvalloissa sijaitsevaan Google Inc.:iin soveltaa EU:n henkilötietodirektiiviä Espanjassa sijaitsevan tytäryhtiö Google Spainin kautta. Tulkintaa kysyttiin myös henkilötietojen käsittelyn ja rekisterinpitäjän määritelmille, sillä epäselvää oli, onko Google rekisterinpitäjä ja onko sen toiminnassa kyse henkilötietojen käsittelystä. Viimeiset ennakkoratkaisukysymykset koskivat varsinaisesti oikeutta tulla unohdetuksi. Ongelmana oli, voidaanko internetin hakukoneita vaatia poistamaan rekisteröityä koskevat henkilötiedot hakutuloksista hänen niin halutessaan, vaikka ne säilyisivät lähdesivulla ja vaikka ne olisi julkaistu laillisesti.[178]

Osa Googlen antamista hakutuloksista on riidattomasti henkilötietoja.[179] Kuten henkilötietojen myös niiden käsittelyn määritelmä on hyvin laaja sekä henkilötietodirektiivissä että tietosuoja-asetuksessa. Googlen itsensä mukaan se ei kuitenkaan käsittele henkilötietoja, koska se ei lajittele niitä muista tiedoista, vaan käsittelee tietoja kokonaisuudessaan.[180] Vastustuksesta huolimatta asiassa oli ilmeistä, että Googlen toiminnassa kyse on henkilötietojen käsittelystä.[181] Oikeastaan kaikkinainen toiminta, jossa henkilötiedot ovat jollain tavalla osallisena, kuuluu henkilötietojen käsittelyn piiriin, joten EUT:n näkemys Googlen toiminnan olevan henkilötietojen käsittelyä ei ollut yllätys.[182]

Googlen mukaan henkilötietodirektiivi ei olisi tullut kuitenkaan sovellettavaksi, sillä Google ei ole rekisterinpitäjä; se ainoastaan lajittelee muiden antamia tietoja täysin automaattisesti ilman tietoa tai määräysvaltaa hakutuloksissa esitetyistä tiedoista.[183] Henkilötietodirektiivin ja nykyisen tietosuoja-asetuksen määritelmät rekisterinpitäjästä ovat identtiset. HTD 2 art. d alakohdan ja TSA 4 art. 7 alakohdan mukaan rekisterinpitäjällä tarkoitetaan

> *”luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot”.*

[178] C-131/12, kohta 20.
[179] C-131/12, kohta 27 ja julkisasiamiehen ratkaisuehdotus C-131/12, kohta 71.
[180] C-131/12, kohta 22.
[181] Julkisasiamiehen ratkaisuehdotus C-131/12, kohta 75, ja C-131/12 kohta 41.
[182] Kulk – Zuiderveen Borgesius 2014, s. 390.
[183] C-131/12, kohta 22.

EUT oli Lindqvist-tapauksessa kuitenkin jättänyt internetin direktiivin soveltamisalan ulkopuolelle suhteellisuusperiaatteeseen vedoten välttääkseen henkilötietodirektiivin liian laajan soveltamisalan.[184] Henkilötietodirektiivi tuli voimaan 1995, jolloin internet oli vasta kehityksensä alkuvaiheessa ja sen merkitys yhteiskunnassa oli huomattavasti vähäisempää. Siten direktiivissäkään ei ollut säännöksiä internetiin liittyen. Teknologian ja tietoyhteiskunnan kehityksen myötä internetin asema on kasvanut huomattavasti, ja henkilötiedoista ja niiden käsittelystä on tullut yhä yleisempää ja tärkeämpää. Samalla henkilötietodirektiivin sanamuodon mukainen soveltamisala on laajentunut paljonkin, mitä EUT pyrki välttämään.

Tähän tukeutuen julkisasiamies katsoi suhteellisuusperiaatteen tulevan kyseeseen Google Spain -tapauksessa, jottei syntyisi kohtuuttomia oikeusvaikutuksia ja jotta lopputulos olisi tasapainoinen.[185] Lisäksi rekisterinpitäjän käsitteen tulkinnassa tulisi huomioida se, että hakukoneen toiminnassa henkilötietoja ei lajitella muista tiedoista. Rekisterinpitäjäksi ja siten myös vastuunkantajaksi tietojen käsittelystä pitäisi katsoa taho, jolla on tosiasiallinen valta tietojen käyttöön.[186] Hakukoneilla ei ole määräysvaltaa tietojen käytöstä, vaan ne toimivat henkilötietojen suhteen passiivisesti olematta edes tietoisia niistä. Haun palveluntarjoajalla ole myöskään minkäänlaista suhdetta lähdesivulla julkaistuun sisältöön. Tämän perusteella internetin hakukoneita ei voitaisi myös suhteellisuusperiaate huomioiden pitää rekisterinpitäjinä, vaikka sanamuodon mukaisesti hakukoneet niiksi määrittyisivätkin.[187] Lisäksi koska hakukoneet eivät voisi turvata henkilötietodirektiivin edellyttämien vaatimusten täyttämistä koskien henkilötietojen laatua ja niiden käsittelyn laillisuutta (HTD 6–8 art.), hakukoneet olisivat suoraan vastoin EU:n oikeutta, jos niitä pidettäisiin rekisterinpitäjinä.[188] Myös Google vetosi suhteellisuusperiaatteeseen, sillä Googlen mukaan lähdesivusto on yksin vastuussa julkaisuistaan. Julkaisijalla olisi myös hakukonetta huomattavasti paremmat mahdollisuudet arvioida julkistamisen laillisuutta sekä tehokkaasti estää kohteena olevien tietojen saatavuutta.[189]

EUT oli kuitenkin eri mieltä edellä esitetyn kanssa. Koska hakukoneet määrittelevät oman toimintansa ja siten samalla myös tekemänsä henkilötietojen käsittelyn tarkoituksen ja kei-

[184] C-101/01, kohdat 67–70.
[185] Julkisasiamiehen ratkaisuehdotus C-131/12, kohdat 30 ja 79.
[186] Julkisasiamiehen ratkaisuehdotus C-131/12, kohdat 72 ja 81–82, ja WP 169, 1/2010 s. 9.
[187] WP 148, 1/2008, s. 14, ja julkisasiamiehen ratkaisuehdotus C-131/12, kohdat 84–88.
[188] Julkisasiamiehen ratkaisuehdotus C-131/12, kohdat 89–90.
[189] C-131/12, kohta 63.

not, EUT katsoi, että jo direktiivin sanamuodon mukaan Google ja muut hakukoneet ovat direktiivin tarkoittamia rekisterinpitäjiä.[190] Sanamuodon lisäksi EUT tukeutui teleologiseen tulkintaan. Henkilötietodirektiivin tavoitteena oli rekisteröityjen tehokas ja kattava suojelu, mikä ei EUT:n mukaan toteutuisi, jos hakukoneita ei katsottaisi rekisterinpitäjiksi, sillä hakukoneiden henkilötietojen käsittely menee pidemmälle kuin lähdesivuilla tietojen julkaiseminen. Hakukoneiden luettelemien tulosten avulla rekisteröidystä voidaan saada suhteellisen tarkka profiili, minkä tekeminen ilman hakukoneita olisi mahdotonta, sillä jo yksittäisten henkilötietojen löytäminen internetistä olisi tällöin huomattavasti hankalampaa. Verrattuna lähdesivuilla tietojen julkaisemiseen internetin hakukoneet vaikuttavat rekisteröityjen yksityisyyteen ja henkilötietojen suojaan selvästi enemmän.[191] Niinpä sekä sanamuodon että mahdollisimman laajan henkilötietojen suojan takaamisen seurauksena hakukoneet katsottiin rekisterinpitäjiksi.

5.1.2. Milloin on oikeus tulla unohdetuksi?

Koska hakukoneet katsottiin rekisterinpitäjiksi, niiden täytyy luonnollisesti kantaa tietosuojanormien rekisterinpitäjille asetettu vastuu, johon kuuluu muun muassa tietosuoja-asetuksen vastaisten tietojen poisto rekisteristä eli oikeuden tulla unohdetuksi toteuttaminen. Google Spain -tapauksessa kysymyksenä oli, millaisissa tilanteissa tietojen poistoa voidaan perustellusti vaatia ja tiedot tulee poistaa.[192] Riittääkö siihen, että rekisteröity ei halua hänen tietojaan käsiteltävän tai hän katsoo tietojen käsittelyn voivan aiheuttaa hänelle vahinkoa?

Julkisasiamiehen mukaan rekisteröidyn halu tietojen poistoon tai niiden mahdollinen vahingollisuus olivat vain subjektiivisia mieltymyksiä, joita ei voitu pitää HTD 14 artiklan tarkoittamina huomattavan tärkeinä ja perusteltuina syinä vastustaa henkilötietojen käsittelyä. Lisäksi La Vanguardia -lehdessä julkaistut tiedot olivat laillisesti julkaistu, joten HTD 12 artiklan mukainen oikeus vaatia tietojen poistoa olisi tullut kyseeseen vain, jos Google olisi käsitellyt henkilötietoja muuten direktiivin vastaisesti.[193] Monet asiassa lausunnon antaneet tahot olivat julkisasiamiehen kannalla ja katsoivat, että oikeus tulla unohdetuksi

[190] C-131/12, kohta 33.
[191] C-131/12, kohdat 34–38.
[192] C-131/12, kohta 20.
[193] Julkisasiamiehen ratkaisuehdotus C-131/12, kohdat 108 ja 105.

on mahdollista vain, kun henkilötietojen käsittely ei ole ollut henkilötietodirektiivin mukaista rekisteröidyn omista toiveista riippumatta.[194]

EUT oli kuitenkin jälleen vahvemmin rekisteröidyn puolella ja käsitti oikeuden tulla unohdetuksi laajemmin. Sen mukaan henkilötietojen käsittelyn yhteensopimattomuus direktiivin kanssa voi johtua tietojen virheellisyyden tai puutteellisuuden lisäksi esimerkiksi siitä, etteivät tiedot ole tarkoituksenmukaisia tai ne ovat liian laajoja tarkoitukseensa. Olosuhteet ovat myös voineet ajan myötä muuttua, jolloin henkilötiedot ovat saattaneet tulla epäolennaisiksi. Siten paikkansapitävienkin tietojen käsittely on vastoin henkilötietodirektiiviä, jos tiedot eivät ole asianmukaisia, olennaisia tai ne ovat liian laajoja suhteessa siihen tarkoitukseen, johon niitä käsitellään. Tapauskohtainen harkinta huomioiden internetin hakukoneen täytyy poistaa edellä mainitun kaltaiset tiedot.[195] Näin ollen rekisteröidyn pelkkä halu ei riittänyt oikeuden vaatimiseen, mutta EUT:n tulkinta henkilötietodirektiivin vastaisesta tietojen käsittelystä oli huomattavasti laajempi kuin muiden asiaan osallistuneiden.

Oikeus tulla unohdetuksi vaatii tapauskohtaista punnintaa, jossa huomioon otetaan rekisteröidyn asema, henkilötietojen paikkansapitävyys, laajuus ja olennaisuus sekä niiden arkaluonteisuus. Mitä kauemman aikaa tietojen julkaisemisesta on, sitä enemmän ne ovat yleensä menettäneet relevanttiuttaan.[196] EUT painotti, että ”oikeuden toteaminen ei edellytä sitä, että kyseessä olevien tietojen sisällyttäminen hakutulosten luetteloon aiheuttaa vahinkoa rekisteröidylle”.[197] Vaara aiheutuvasta vahingosta kuitenkin vahvistaa perusteita poistaa mahdollista vahinkoa aiheuttavat tiedot.[198] Poistettavaksi vaadittavien henkilötietojen tulee myös olla luonteeltaan yksityisiä, sillä oikeuden tulla unohdetuksi perustana on POK 8 artiklan henkilötietojen suojan lisäksi myös POK 7 artiklassa säädetty yksityiselämän suoja. EUT perusteleekin ratkaisuaan myös tietojen arkaluonteisuudella.[199]

Tietosuoja-asetuksen tarkoitus on entisestään laajentaa oikeutta tulla unohdetuksi.[200] Siitä säädetään nimenomaisesti TSA 17 artiklassa, jonka 1 kohdan mukaan rekisteröidyllä on oikeus saada rekisterinpitäjä poistamaan rekisteröidyn henkilötiedot, jos niitä ei enää tarvita niihin tarkoituksiin, joita varten ne on kerätty, tai jos rekisteröity peruuttaa antamansa

[194] C-131/12, kohta 90.
[195] C-131/12, kohdat 92–94.
[196] Ks. WP 225, s. 13–20.
[197] C-131/12, kohta 96.
[198] WP 225, s. 18.
[199] C-131/12, kohta 97–99.
[200] TSA:n johdanto, kohta 66.

suostumuksen, johon käsittely on perustunut. Niinpä nykyisin rekisteröidyn pelkkä halu tietojen poistoon riittää perusteeksi, kunhan käsittely on alkujaan perustunut rekisteröidyn antamaan suostumukseen. Lisäksi poistoa voidaan TSA 17(1) artiklan mukaan vaatia mahdollisen lakisääteisen velvoitteen noudattamiseksi tai jos käsittely on ollut lainvastaista taikka jos rekisteröity vastustaa käsittelyä eikä rekisterinpitäjällä ole huomattavan tärkeää ja perusteltua, rekisteröidyn oikeuden syrjäyttävää syytä käsittelylle.

Vaikka jokin edellä mainituista perusteista täyttyisikin, TSA 17(3) art. mukaan oikeutta tulla unohdetuksi ei ole, kun on kyse sananvapautta ja tiedonvälityksen vapautta koskevan oikeuden käyttämisestä. Samoin oikeutta tulla unohdetuksi ei ole, jos asiassa kyse on kansanterveyteen liittyvistä yleistä etua koskevista syistä, oikeudellisen vaateen laatimisesta, esittämisestä tai puolustamisesta tai yleisen edun mukaisista arkistointitarkoituksista ja tieteellisistä, historiallisista tai tilastollisista tutkimustarkoituksista. Oikeutta ei ole myöskään, kun rekisterinpitäjän täytyy lakisääteinen velvollisuuden, yleistä etua koskevan tehtävän suorittamisen tai julkisen vallan käyttämisen takia käsitellä rekisteröidyn henkilötietoja.

Erityisesti sanan- ja tiedonvälityksen vapautta koskeva poikkeus tulee kyseeseen hakukoneiden kohdalla. Joutuessaan tekemään eri oikeuksien välistä punnintaa Googlesta ja muista hakukoneista on tullut ensisijaisia tahoja, jotka määrittelevät sanan- ja tiedonvälityksen vapauden suhteen yksityisyyteen ja henkilötietojen suojaan internetissä. Tätä on kritisoitu, sillä tehtävän on katsottu rinnastuvan viranomaistoimintaan ja olevan myös erittäin haastavaa.[201] Hakukoneiden ollessa voittoa tavoittelevia yrityksiä peloksi nousi, että ne eivät taloudellisen tehokkuuden takia suorittaisi kunnollista punnintaa vaan poistaisivat kaiken pyydetyn, jolloin sananvapautta ja tiedonsaantia rajoitettaisiin täysin perusteetta ja yksityinen ihminen voisi hakukoneen kautta sensuroida julkaisuja.[202] Samalla syntyisi riski internetin aseman heikentymisestä vapaana tiedonvälittäjänä.[203] Aiheellisesta huolesta huolimatta vaikuttaisi siltä, että ainakin Google pyrkii tekemään EUT:n edellyttämää tapauskohtaista arviointia, sillä tämän hetkisten tilastojen mukaan Google hylkää sille tehdyistä poistopyynnöistä 56 %.[204] Siten pelättyä linkkien massapoistoa ei ole tapahtunut.

[201] Ek 2014, s. 120, Jones 2014, s. 600 ja Kuner 2015, s. 18.
[202] Julkisasiamiehen ratkaisuehdotus C-131/12, kohdat 133–134, ja Jones 2014, s. 599.
[203] Jones 2014, s. 599.
[204] https://transparencyreport.google.com/eu-privacy/overview

5.2. Oikeuden tulla unohdetuksi globaali ulottuvuus

5.2.1. EU:n tietosuojanormien alueellinen soveltamisala

Google Spain -tapauksessa ongelmaksi nousi henkilötietodirektiivin alueellinen soveltamisala: voitiinko direktiivin täytäntöönpanevaa kansallista oikeutta soveltaa myös EU:n ulkopuolelle sijoittautuneisiin toimijoihin, kuten Google Inc.:iin? Google Inc. on Googlen maailmanlaajuisen konsernin emoyhtiö, ja sen koti paikka on Yhdysvalloissa. Yhtiö on perustanut eri puolille maailmaa tytäryhtiötä, esimerkiksi Google Spainin Espanjaan, edistämään ja markkinoimaan Googlen mainostuotteiden ja -palvelujen myyntiä kyseisissä maissa.[205] HTD 4(1) artiklan mukaan direktiivin perusteella annettua kansallista lainsäädäntöä sovellettiin, kun henkilötietojen käsittely suoritettiin jäsenvaltion alueella sijaitsevassa rekisterinpitäjän toimipaikassa tapahtuvan toiminnan yhteydessä. Samoin direktiiviä sovellettiin, kun rekisterinpitäjä oli sijoittautunut paikkaan, jossa sovellettiin jäsenvaltion kansallista lakia kansainvälisen julkisoikeuden nojalla taikka kun EU:n alueelle sijoittautumaton rekisterinpitäjä käytti henkilötietojen käsittelyssä välineitä, jotka sijaitsivat kyseisen jäsenvaltion alueella. Ratkaisevaa oli rekisterinpitäjän sijoittautumispaikka tai käsittelyssä käytettyjen välineiden ja keinojen sijainti, eikä henkilötietojen fyysisellä sijainnilla ei ollut merkitystä. [206]

Google Spain kuului riidattomasti espanjalaisen lain piiriin sijoittautuessaan Espanjaan. Sen tehtävänä on kuitenkin vain mainospaikkojen markkinointi ja myynti, eikä sillä ole mitään tekemistä itse henkilötietojen käsittelyssä tai hakukoneen ylläpidossa. Tästä syystä Google väitti, ettei EU:n lainsäädäntöä voitu soveltaa Google Inc.:iin, joka on vastuussa sekä henkilötietojen käsittelystä että hakukoneen toiminnasta sen kuuluessa Yhdysvaltojen lain alle.[207] Merkitystä ei kuitenkaan ollut henkilötietojen varsinaisella käsittelijällä tai käsittelypaikalla, koska toimipaikan ei itse edellytetty suorittavan käsittelyä,[208] vaan ratkaisevaksi muodostui ilmaus ”toimipaikassa tapahtuvan toiminnan yhteydessä”. Koska Google Spainin avulla Googlen toiminnasta pyrittiin tekemään taloudellisesti kannattavaa sen myydessä ja markkinoidessa Googlen mainospaikkoja, emoyhtiön ja tytäryhtiön toimintojen katsottiin liittyvän erottamattomasti toisiinsa. Tällöin kyse on EU:ssa sijaitsevan toimipaikan toiminnan yhteydessä tapahtuvasta henkilötietojen käsittelystä riippumatta

[205] C-131/12, kohta 43.
[206] WP 179, 8/2010, s. 8.
[207] C-131/12, kohta 51.
[208] C-131/12, kohta 52.

tosiasiallisen käsittelijän sijainnista, joten tapauksessa voitiin soveltaa henkilötietodirektiiviä.[209]

Lopputulema oli perusteltu, sillä ilman eri maihin sijoittautuneita tytäryhtiöitään Googlen hakukoneen toiminta ei olisi välttämättä taloudellisesti kannattavaa, mikä puolestaan on elinehto yhtiön toiminnalle. Lisäksi henkilötietodirektiivin mukaan ”tietojenkäsittelyä suorittavan sijoittautuminen kolmanteen maahan ei saa olla esteenä tässä direktiivissä säädetylle yksilöiden suojalle”.[210] Mikäli Google olisi jäänyt soveltamisalan ulkopuolelle, rekisteröityjen tehokas ja kattava perusoikeuksien suoja olisi kärsinyt.[211] EU:n näkökulmasta alueellisen soveltamisalan suppeampi tulkinta ei ollut vaihtoehto, koska muutoin tietosuojasäännösten kiertäminen olisi ollut helppoa. Internetin mahdollistaessa sijainnista riippumattoman globaalin toiminnan kolmansiin maihin sijoittautuneet yritykset olisivat voineet toimia esimerkiksi konsernin avulla EU:n alueella noudattaen eri tietosuojalainsäädäntöä kuin EU:n alueelle sijoittautuneet. Tämä olisi aiheuttanut henkilötietojen suojan heikentymisen mutta myös asettanut unionin alueelle sijoittautuneet yritykset heikompaan asemaan niiden joutuessa noudattamaan tiukempia säännöksiä kuin mitä muualle sijoittautuneiden yritysten olisi täytynyt.

Tietosuoja-asetuksen alueellista soveltamisalaa sääntelevässä 3 artiklassa on vastaava ilmaus toimipaikassa toiminnan yhteydessä tapahtuvasta henkilötietojen käsittelystä. Säännöstä on kuitenkin tarkennettu edeltäjästään säätämällä nimenomaisesti, ettei sillä ole merkitystä, missä henkilötietojen käsittely varsinaisesti tapahtuu. Uuteen asetukseen on siten sisällytetty EUT:n edellä kerrottu linjaus. Tietosuoja-asetuksen alueellinen soveltamisala on muutenkin laajempi kuin henkilötietodirektiivin. Aikaisemmin EU:n tietosuojalainsäädännössä sen ylivaltaa pidettiin oletuksena, mutta uudessa tietosuoja-asetuksessa on siirrytty kohti suunniteltua ylivoimaa.[212] TSA 3 artiklan mukaan

> *1. Tätä asetusta sovelletaan henkilötietojen käsittelyyn, jota suoritetaan unionin alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toiminnan yhteydessä, riippumatta siitä, suoritetaanko käsittely unionin alueella vai ei.*

[209] C-131/12, kohdat 55–56 ja 60. Ks. myös julkisasiamiehen ratkaisuehdotus C-131/12, kohta 67.
[210] HTD johdanto, kohta 20.
[211] C-131/12, kohdat 54 ja 58.
[212] Lynskey 2015, s. 41 ja 44.

2. Tätä asetusta sovelletaan unionissa olevia rekisteröityjä koskevien henkilötietojen käsittelyyn, jota suorittava rekisterinpitäjä tai henkilötietojen käsittelijä ei ole sijoittautunut unioniin, jos käsittely liittyy

a) tavaroiden tai palvelujen tarjoamiseen näille rekisteröidyille unionissa riippumatta siitä, edellytetäänkö rekisteröidyltä maksua; tai

b) näiden rekisteröityjen käyttäytymisen seurantaan siltä osin kuin heidän käyttäytymisensä tapahtuu unionissa.

3. Tätä asetusta sovelletaan henkilötietojen käsittelyyn, jota suorittava rekisterinpitäjä ei ole sijoittautunut unioniin vaan toimii paikassa, jossa sovelletaan jonkin jäsenvaltion lakia kansainvälisen julkisoikeuden nojalla.

Alueellinen soveltamisala laajenee 2 kohdan seurauksena huomattavasti, koska tietosuoja-asetuksen sovellettavaksi tuleminen ei enää edellytä rekisterinpitäjällä olevan EU:ssa mitään toimipaikkaa. Ainoastaan se riittää, että rekisteröity on unionissa ja hänelle tarjotaan tavaraa tai palvelua tai hänen käyttäytymistään EU:n alueella seurataan. Vaikka EU:ssa oleskelevilla on internetin kautta pääsy minne tahansa verkkokauppaan ja mahdollisuus saada palveluja mistä vain, se ei kuitenkaan riitä perusteeksi asetuksen soveltamiseen. Rekisterinpitäjä tulee tarjota tavaroita tai palveluja nimenomaan unionin markkinoille. Tarjoamisesta on kyse, kun tuotetta tai palvelua esimerkiksi mainostetaan EU:ssa. Arvioinnissa huomioidaan myös esimerkiksi, mitä kieltä tai valuuttaa tilauksessa on mahdollista käyttää tai jos tavaran tai palvelun tarjoaja mainitsee EU:ssa olevista asiakkaistaan.[213] Nähdäkseni mahdollisuus käyttää valuuttana euroa tai muuta EU-jäsenmaan valuuttaa indikoi suoraan palvelun tai tavaran tarjoamisen kohdistuvan EU:hun, mutta kielten osalta englannin, ranskan tai espanjan käyttäminen ei vielä tarkoita EU:n alueelle kohdistuvaa tarjoamista kyseisten kielten ollessa yleisiä laajalti muuallakin. Toisin on esimerkiksi saksan tai suomen kohdalla, jolloin suuntautuminen EU:n markkinoille on selvää.

Vaikka jo Google Spain -tapauksen jälkeen on ollut selvää, että EU:n tietosuojanormeja voidaan soveltaa Googlen ja myös muiden hakukoneiden toimintaan, tietosuoja-asetus vahvistaa tätä entisestään, sillä soveltaminen voi tapahtua nykyään joko TSA 3(1) tai TSA 3(2) a alakohdan mukaan. Sen sijaan osittain epäselvää on, keiden rekisteröityjen suhteen asetus tulee sovellettavaksi. SEUT 16 artiklan ja POK 8 artiklan mukaan *jokaisella* on oi-

[213] TSA johdanto, kohta 23.

keus henkilötietojen suojaan. Samoin tietosuoja-asetuksessa todetaan, että yksilöiden oikeus henkilötietojen suojaan on huomioitava kansalaisuudesta tai asuinpaikasta riippumatta.[214] Lisäksi TSA 3(2) artiklassa puhutaan unionissa olevista rekisteröidyistä eli henkilöistä, jotka fyysisesti ovat EU:n rajojen sisäpuolella.[215]

Tämän perusteella EU:n normeja sovelletaan myös henkilöihin, joilla ei ole varsinaisesti mitään sidettä EU:hun, vaan he ovat esimerkiksi turisteja. Siten voi olla mahdollista, että asetusta sovelletaan kolmannesta maasta tulevan rekisteröidyn ja kolmanteen maahan sijoittautuneen rekisteripitäjän väliseen suhteeseen, kunhan rekisteröity on EU:n alueella. Tällaisessa tilanteessa ilmenee EU:n vahva kapasiteetti luoda alueestaan ihmisoikeuksille pyhitetty alue. EU voi vaikuttaa sille periaatteessa täysin ulkopuolisten välisiin suhteisiin, kun toisena osapuolena on ihmisoikeuksilla suojattava yksilö, joka on fyysisesti astunut EU:n tarjoaman suojan piiriin.

SEUT 16 ja POK 8 artikloista huolimatta rekisteröidyltä on kuitenkin aiemmin vaadittu jonkinlaista yhteyttä EU:hun. Tällaiseksi on katsottu esimerkiksi kansalaisuus tai oleskelulupa, jotta oikeutta tulla unohdetuksi on voitu vaatia, vaikka myös henkilötietodirektiivin johdannossa henkilötietojen suojan on todettu kuuluvan jokaiselle.[216] Suhteellisuusperiaatteen perusteella on mahdollista, että aiempi ohjeistus katsotaan edelleen paikkansa pitäväksi ja yhteys EU:hun vaaditaan tietosuoja-asetuksenkin kohdalla, jolloin tietosuojaturismi ei onnistuisi. Samalla kuitenkin päädytään absurdiin tilanteeseen: Rekisterinpitäjän täytyy noudattaa tietosuoja-asetusta sen tullessa sovellettavaksi jo perussopimusten nojalla, mutta rekisteröity ei voisi vaatia itselleen asetuksessa rekisteröidyille turvattuja oikeuksia.

Joka tapauksessa on selvää, että valtaosalla EU:ssa olevista ihmisistä on oikeus vaatia Googlelta tai muilta hakukoneilta heitä koskevien linkkien poistamista. Edellä käsitellyt normit alueellisesta soveltamisalasta eivät kuitenkaan kerro, missä laajuudessa itse linkkien poisto tulee tehdä ja ulottuuko hakukoneen poistovelvollisuus myös kolmansissa maissa näytettäviin hakutuloksiin. Google Spain -ratkaisu jäi siten hieman puolitiehen, sillä EUT ei ottanut lainkaan kantaa tähän ongelmaan.

---

[214] TSA johdanto, kohdat 2 ja 14.
[215] Eri kieliversiot käyttävät samaa ilmausta; esim. ”data subjects who are in the Union”, ”Personen, die sich in der Union befinden”, ”des personnes concernées qui se trouvent sur le territoire de l'Union” ja ”registrerade som befinner sig i unionen”.
[216] WP 225, s. 3, ja HTD johdanto, kohta 2. Myös sekä Googlen että Bingin tietojenpoistopyyntölomakkeissa on ilmoitettava EU:hun kuuluva asuin- tai alkuperämaa. https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=0-636663760383976871-1219462126&rd=1 ja https://www.bing.com/webmaster/tools/eu-privacy-request

5.2.2. Oikeuden tulla unohdetuksi ekstraterritoriaalisuus

Kun rekisteröity on tehnyt menestyksekkään pyynnön linkkien poistamiseksi, hänen tietonsa eivät kuitenkaan katoa internetistä, sillä hakukoneille tehdyt poistopyynnöt koskevat vain niiden hakutuloksissaan näyttämiä linkkejä. Henkilötiedot ovat edelleen lähdesivulla, ellei sillekin ole tehty pyyntöä tietojen poistamisesta. On myös mahdollista, että lähdesivulta on kopioitu tietoja muualle internetiin. Yleisesti tunnustettu tosiasia on, että mikä on kerran laitettu internetiin, on mahdotonta saada sieltä pois. Kuten EUT Google Spain -tapauksessa totesi, hakukoneilla on kuitenkin merkittävä osuus henkilön näkyvyydelle internetissä. Tästä johtuen sillä on merkitystä, kuinka laajasti linkkien poistaminen tehdään vai onko rajaaminen edes mahdollista.

Kuten luvussa 4.2.2. havaittiin, henkilötietojen suojassa yleisesti edellytykset Brysselefektin toteutumiseen täyttyvät. Efektin toteutuminen oikeuden tulla unohdetuksi kohdalla internetin hakukoneissa on kuitenkin riippuvainen hakukoneiden tosiasiallisesta toiminnasta ja sääntelyn kohteen jaettavuudesta tai jakamattomuudesta. Vaikka yleensä EU:n tietosuojalainsäädännön alaisuuteen kuuluvien henkilötietojen erottaminen muista henkilötiedoista on joko täysin mahdotonta tai muuten kannattamatonta, hakukoneiden antamien linkkien kohdalla asia on eri. Siinä oikeuden tulla unohdetuksi kohde tarkoittaa yksittäisiä linkkejä, joita koskien poistopyyntö tehdään. Esimerkiksi Googlella on monia kansallisia verkkotunnuksia[217], joiden kautta tehdyistä hauista pyydetyt linkit voidaan poistaa, mutta silti näyttää hauissa, jotka tehdään toisessa verkkotunnuksessa. Siten näytettävien hakutulosten jaottelu verkkotunnusten avulla EU:hun ja kolmansiin maihin onnistuu helposti, jolloin oikeus tulla unohdetuksi voidaan kohdistaa vain EU:n jäsenmaiden kansallisiin verkkotunnuksiin. Teknisesti hakukoneiden on myös mahdollista hallita hakutuloksissa annettavia linkkejä maantieteellisesti IP-osoitteen[218] perusteella tehtävän maarajoituksen avulla. Tällöin käytetystä verkkotunnuksesta riippumatta EU:ssa olevat internetin käyttäjät voidaan tunnistaa ja estää heitä saamasta hakutuloksiinsa EU:n tietosuojalainsäädännön perusteella poistettuja linkkejä. Tämä tarkoittaa, että hakukoneiden on ilman lisäkustannuksia mahdollista poistaa pyydetty linkki hakutuloksista koskien vain EU:ta, jolloin Brys-

[217] Verkkotunnus eli domain tarkoittaa internetsivun osoitetta. Verkkotunnus muodostuu pääosasta ja päätteestä, joita ovat esim. .com ja kansalliset .fi ja .se.
[218] IP-osoite tarkoittaa numerosarjaa, jolla voidaan yksilöidä verkkosovitin, joka puolestaan tarkoittaa tietokoneen internetiin liittävää laitetta.

sel-efekti ei toteudu lainkaan muiden edellytysten täyttymisestä huolimatta. Ja juuri näin ainakin Google toimii.[219]

Koska Bryssel-efekti ei ole toteutunut oikeuden tulla unohdetuksi kohdalla, EUT on kohdannut jo edellä mainitun ongelman oikeuden globaalista laajuudesta. Ranskan Conseil d'État on tehnyt EUT:lle ennakkoratkaisupyynnön koskien Google Inc.:n ja Ranskan tietosuojaviranomaisen CNIL:n (Commission nationale de l'informatique et des libertés) välistä kiistaa siitä, ulottuuko oikeus tulla unohdetuksi globaalisti kaikkialle maailmaan vai tuleeko sen toteutuminen taata ainoastaan EU:n alueella.[220] Asiassa Google on hyväksynyt rekisteröidyn pyynnön häntä koskevien linkkien poistamisesta, mutta kysymyksenä on, täytyykö linkit poistaa globaalisti niin, etteivät ne näy enää lainkaan riippumatta haun tekopaikasta, ja koskeeko poistovelvollisuus kaikkia verkkotunnuksia.[221] Asiassa on kysytty henkilötietodirektiivin tulkintaa, sillä tietosuoja-asetus on tullut sovellettavaksi vasta ennakkoratkaisupyynnön tekemisen jälkeen. Asetuksessakaan ei sen paremmin ole kuitenkaan tuotu ilmi, onko oikeuden tulla unohdetuksi tarkoitettu olevan globaali.

Vaikka internet ei tunne rajoja, kansalliset verkkotunnukset tavallaan vastaavat kyseisiä kansallisvaltioita internetissä. Näin ajateltuna oikeuden tulla unohdetuksi on katsottu ulottuvan EU:n rajojen ulkopuolelle, sillä hakukoneen tulisi poistaa tiedot "kaikista relevanteista verkkotunnuksista mukaan lukien .com" eikä vain EU:n jäsenvaltioiden kansallisista verkkotunnuksista.[222] Vain vähän jälkeen Google Spain -tuomion rajoitettua tiedonsaantia pystyi kiertämään helposti, sillä poistetut tiedot olivat saatavilla esimerkiksi google.com:n kautta.[223] Kuten edellä kävi ilmi, nykyisin hyväksyessään rekisteröidyn poistopyynnön Google poistaa tiedot eurooppalaisista verkkotunnuksista sekä käyttää maantieteellistä rajoitusta, jolloin EU:hun kuuluvasta IP-osoitteesta tehdyssä haussa ei näy poistettuja tietoja riippumatta käytetystä Googlen verkkotunnuksesta. Samoin Bing-hakukoneen tietojenpoistolomakkeessa puhutaan hakutulosten rajoittamisesta vain Euroopassa.[224]

Teknologia vaikuttaa olevan aina askeleen lainsäädäntöä edellä, sillä esimerkiksi maantieteellisen rajoituksen kiertäminen onnistuu huijaamalla IP-osoitteen tulevan jostain muusta maasta, kuin mikä se oikeasti olisi. Tällä tavalla EU:nkin alueella voi päästä käsiksi pois-

[219] https://support.google.com/transparencyreport/answer/7347822
[220] Asia C-507/17.
[221] EUVL C 347, s. 23.
[222] WP 225, s. 3.
[223] Ek 2014, s. 121.
[224] Ks. https://www.bing.com/webmaster/tools/eu-privacy-request

tettuihin tietoihin. CNIL:n mukaan Googlen toimet eivät ole riittäviä, vaan oikeuden tulla unohdetuksi tulisi toteutua globaalisti, jottei myöskään kolmansissa maissa tehdyissä hauissa näkyisi linkkien poistamispyynnön tehneen henkilötietoja. Muussa tapauksessa oikeus tulla unohdetuksi ei toteutuisi *de facto*. Google vastustaa EU:n lainsäädännön mahdollista globaalia ulottuvuutta, sillä tällöin voi ensinnäkin syntyä ristiriitoja, jos muutkin valtiot katsovat voivansa vaatia Googlelta globaaleja toimia, ja toisekseen EU:n lainsäädäntöä noudattaessaan Google voisi joutua rikkomaan kolmannen maan lainsäädäntöä etenkin sananvapauteen ja tiedonvälitykseen liittyen.[225]

Google on kohdannut vaatimuksia hakutulosten rajoittamisesta globaalisti aiemminkin. Vuonna 2017 Kanadan korkein oikeus velvoitti Googlen poistamaan linkit globaalisti tapauksessa, jossa yritys teki laitonta liiketoimintaa internetin kautta toisen yrityksen immateriaalioikeuksia käyttäen.[226] Google vastusti oikeuden antamaa määräystä, sillä sen globaali noudattaminen voisi rikkoa jonkun toisen valtion lakia ja lainkäyttövaltaa, kun taas tuomioistuin katsoi, ettei loukatun yrityksen oikeuksia voitu internetissä muuten suojata.[227] Vaikka kyse ei ollut oikeudesta tulla unohdetuksi ja sananvapaudesta, tilanne on analogisesti samanlainen kuin edellä puhutussa ennakkoratkaisupyynnössä, ja Googlen vasta-argumentit ovat samat molemmissa tapauksissa. Google on oikeassa perustellessaan vastustamistaan mahdollisilla ristiriidoilla eri maiden lainkäyttövallan välillä. Se on jo toteutunut kalifornialaisen piirioikeuden vapauttaessa Googlen noudattamasta Kanadan korkeimman oikeuden edellä mainittua määräystä linkkien globaalista poistamisesta[228] — tosin Googlen itsensä tekemän haasteen johdosta saadakseen suotuisan tuomion, jonka avulla se voi vaatia kanadalaisen tuomioistuimen rajoittamaan määräyksen globaalia ulottuvuutta.

Asiassa C-507/17 EUT on puun ja kuoren välissä. Mikäli EUT katsoo, että hakukoneen on toteutettava linkkien poisto hakutuloksista globaalisti, se tunkeutuu kolmansien maiden lainkäyttövallan piiriin pakottaessaan hakukoneet noudattamaan EU:n lainsäädäntöä maailmanlaajuisesti ja rajoittaa ihmisten tiedonsaantia, joilla ei ole mitään yhteyttä unioniin. Jos EUT taas ei ulota oikeutta tulla unohdetuksi globaaliksi koskien kaikkia verkkotunnuksia, kyseisen oikeuden toteutuminen jää vain haaveeksi, sillä henkilötiedot pysyvät kol-

[225] https://www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed
[226] 2017 SCC 34, Google Inc. v. Equustek Solutions Inc.
[227] 2017 SCC 34, kohdat 44 ja 41.
[228] N.D. Cal. No. 5:17-cv-04207-EJD, Google LLC v. Equustek Solutions Inc.

mansissa maissa edelleen saatavilla. Lisäksi maarajoituksia kiertämällä poistettavaksi vaaditut tiedot ovat saatavissa myös EU:ssa. Tällöin EU:n oman sääntelyn ja sen takaamien oikeuksien toteutumista ei voitaisi turvata edes sen omalla alueella.

Ennakkoratkaisupyyntö osoittaa loistavasti, kuinka internetiä on hankala säännellä sen kuuluessa kaikkien valtioiden lainkäyttövaltaan ja samalla ollessa kaikkien ulottumattomissa. Oli EUT:n ratkaisu mikä tahansa, on erittäin epätodennäköistä, että Google jättäisi EU:n markkinat. EUT:n vaatiessa globaalia oikeutta tulla unohdetuksi Google joko noudattaa EU:n lainsäädäntöä maailmanlaajuisesti tai todennäköisemmin toimii samoin kuin edellä Kanadan korkeimman oikeuden antamaa määräystä vastaan. Tämä tarkoittaa, että se veisi asian kolmannen maan, luultavasti ainakin yhdysvaltalaiseen tuomioistuimeen, joka mahdollisesti vapauttaa Googlen linkkien poistovelvollisuudesta perustuen kyseisen valtion lainsäädäntöön. Seurauksena on kova kilpailu eri tuomioistuinten toimivallasta ja siitä, kuka saa sanoa viimeisen sanan internetissä olevan tiedon suhteen. Esimerkiksi Yhdysvalloissa on ollut hyvin eri näkemys hakukoneen velvollisuudesta poistaa linkkejä hakutuloksista kuin EU:ssa,[229] ja kyseinen linja jatkuu edelleen. Suvereenien valtioiden ja EU:n ylimpien oikeusasteiden tuomioiden välisiä ristiriitoja on mahdotonta ratkaista niiden tunkeutuessa toistensa alueelle. Kuitenkin mitä paremmin EUT toisi päätöksissään perustelut ja syyt sekä olennaiset seikat globaalille vaikutukselle, sitä enemmän niitä voitaisiin hyväksyä ja kunnioittaa kolmansissa maissa.[230] Silti on toiveajattelua, että näkemysten ollessa vastakkaiset, pelkästään EUT:n paremmat perustelut ratkaisisivat kiistan.

[229] Cate 1998, s. 73.
[230] Kuner 2015, s. 21.

6. Henkilötietojen siirto

Edellä tarkasteltu oikeus tulla unohdetuksi kuvastaa hyvin rekisteröidylle annettua kontrollivaltaa, henkilötietojen korkeatasoista suojaa sekä niiden kiinteää yhteyttä yksityisyyteen. Sen sijaan henkilötietojen taloudellinen merkitys ei siinä juuri erotu. Seuraavaksi tarkastellaankin EU:n tietosuojasääntelyn ekstraterritoriaalisuutta henkilötietojen siirron kautta, jossa henkilötietojen yhteys markkinoihin ja talouselämään on huomattavan vahva. Samalla se kuvastaa tietosuoja-asetuksen kaksoistavoitetta, minkä takia ensin käsitellään lyhyesti henkilötietojen siirtoa EU:n sisämarkkinoilla. Toisin kuin oikeudessa tulla unohdetuksi, henkilötietojen siirtojen sääntelyssä on jo lähtökohtaisesti huomioitu henkilötietojen globaali konteksti. EU:n sisäiset henkilötietojen siirrot on tietosuoja-asetuksessa erotettu kolmansiin maihin tapahtuvista siirroista. Tätä kautta lukija saa vertailukohdan luvun jälkimäisessä osassa puheena oleviin rajatylittäviin henkilötietojen siirtoihin. Se myös tarjoaa näkökulman edellä esitettyyn väitteeseen EU:n pyrkimyksistä parantaa tietosuojalainsäädännöllään omaa kilpailuetuaan, koska ekstraterritoriaalisella tietosuojasääntelyllään EU voi tehokkaasti estää tietojen siirron ja siten vaikeuttaa kolmansien maiden yritysten toimintaa.

6.1. Henkilötietojen siirto EU:ssa

6.1.1. Henkilötietojensiirron merkitys

Henkilötietojen korkeatasoisen suojan lisäksi tietosuoja-asetuksen toisena tavoitteena on tehostaa henkilötietojen siirtoa vahvistamalla säännöt henkilötietojen vapaasta liikkuvuudesta (TSA 1(1) art.). Henkilötietojen siirtäminen on talouden kannalta tärkeää, koska niiden merkitys yhteiskunnassa ja yritysten toiminnassa ja siten myös EU:n sisämarkkinoilla on kasvanut huomattavasti. Informaatio on nykyisin maailmantalouden uusi raaka-aine, ja globalisaation myötä henkilötietojen siirto on yritysten toiminnalle usein elinehto.[231]

Tietosuoja-asetusta edeltänyt henkilötietodirektiivi säädettiin juuri sisämarkkinoilla tapahtuvan henkilötietojen tehokkaan siirrettävyyden turvaamiseksi.[232] Jo direktiivissä ollutta tavoitetta on kuitenkin haluttu vahvistaa entisestään, sillä sitä kautta EU:n sisämarkkinoiden toimivuutta ja integraatiota voidaan parantaa henkilötietojen tullessa yrityksille yhä tärkeämmiksi. Vaikka jo direktiivi yhtenäisti jäsenmaiden lainsäädäntöä, jokainen jäsen-

[231] Kuner 2012, s. xi ja 152.
[232] Salbu 2002, s. 669. Ks. myös HTD 1 art.

valtio oli implementoinut henkilötietodirektiivin säännökset hieman eri tavoin. Tästä aiheutui hankaluuksia henkilötietojen siirrossa, kun yhteisestä direktiivistä huolimatta säännöt olivat toisistaan poikkeavia. Niinpä haluttiin asetuksentasoinen sääntely, jolla voidaan varmistaa, että jäsenvaltioiden välillä ei ole tietosuojalainsäädännössä henkilötietojen vapaata liikkuvuutta estäviä eroavaisuuksia.[233]

EU:n sisämarkkinoilla vallitsee neljä vapautta: ihmisten, palveluiden, tavaroiden ja pääoman vapaa liikkuvuus. Tietosuoja-asetuksen pyrkimys henkilötietojen vapaaseen liikkuvuuteen ei kuitenkaan kuulu minkään edellä mainittujen kategorioiden alle, sillä henkilötiedoissa kyse ei ole tavarasta eikä palvelusta. Henkilötietoja voitaisiin pitää eräänlaisena pääomana, mutta sen arvoa on hankala määrittää ja samat tiedot todennäköisesti ovat usean muun tahon hallussa, mikä ei perinteisen pääoman kohdalla tule kyseeseen. Ajatus henkilötietojen ja ylipäätään myös muun datan vapaasta liikkuvuudesta sisämarkkinoiden viidentenä vapautena ei ole kaukaa haettu.[234] Myös EU:n oikeuskomissaari Viviane Reding on nähnyt asian samankaltaisesti todetessaan, että eurooppalaisten työskennellessä, matkustaessa ja käydessä kauppaa vapaasti EU:ssa myös heidän henkilötietojensa tulee liikkua vapaasti.[235]

Henkilötiedot ovat yrityksille välttämättömiä esimerkiksi asiakasrekistereiden ylläpitämiseksi tai palvelujen toimittamiseksi, mutta niistä on yrityksille hyötyä myös mainonnan kohdentamisessa. Kuluttajien kiinnostuksenkohteiden, käyttäytymisen ja elämäntilanteen tietäminen helpottaa vaikuttavan mainonnan luomisessa ja mahdollistaa yksilöllisen mainonnan. Henkilötietojen vapaa liikkuvuus tuo tähän uusia mahdollisuuksia. Samalla se on myös itse asiassa uhka sille, koska tietosuoja-asetuksessa on haluttu myös toisenlaista henkilötietojen vapaata liikkuvuutta: asetus antaa tietyissä tilanteissa rekisteröidylle oikeuden vaatia tietojensa siirtämistä toiseen järjestelmään (TSA 20 art.). Tiedon kerääminen ja analysoiminen ei välttämättä ole enää kannattavaa, kun uhkana on, että toinen taho pääsee hyötymään ensimmäisen toimijan työn hedelmistä. Henkilötietojen käyttö kohdistettuun mainontaan voi vähentyä ja mainonnasta tulla enemmän kontekstiriippuvaista.[236] Tästä

[233] TSA johdanto, kohdat 9–10, 13.
[234] Ks. esim. https://e-estonia.com/free-movement-of-data-as-the-5th-fundamental-freedom-of-the-european-union/
[235] http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm "Europeans live, work, shop and travel freely in the EU, so their data must travel freely as well: Freely and safely."
[236] https://hbr.org/2018/05/how-gdpr-will-transform-digital-marketing

huolimatta henkilötietojen vapaa liikkuvuus unionissa on joka tapauksessa hyvin suuri etu yrityksille ja edistää niiden toimintaa.[237]

6.1.2. Kaksoistavoitteen ristiriita?

Henkilötietojen siirtämisen rajoittaminen tai estäminen, joka perustui henkilötietojen parempaan suojaan, oli HTD 1(2) artiklassa kielletty. Henkilötietodirektiivi painotti enemmän sisämarkkinoita, kun taas tietosuoja-asetuksessa on siirrytty vahvemmin perusoikeuksien puolelle eli henkilötietojen ja yksityisyyden suojaamiseen.[238] Painotuksen muutoksesta huolimatta sisämarkkinoiden integraatio ja tehokas toimivuus on säilynyt tietosuoja-asetuksen lähtökohtana. Asetuksessa on nimittäin HTD 1(2) artiklaa vastaava kohta. TSA 1(3) artiklan mukaan henkilötietojen vapaata liikkuvuutta unionin sisällä ei saa rajoittaa eikä kieltää syistä, jotka liittyvät luonnollisten henkilöiden suojeluun henkilötietojen käsittelyssä. Jäsenmaat eivät siten saa estää tai rajoittaa henkilötietojen siirtoa EU:n sisällä perustellen sitä henkilötiedoille annettavalla suojalla tai oikeudella yksityisyyteen. Tietosuoja-asetus asettaa jokaiselle jäsenvaltiolle samat vaatimukset henkilötietojen suojaan, mutta samalla se estää kansallisen sääntelyn, jolla taattaisiin vielä parempi suoja.

Tietosuoja-asetuksen tavoitteet vaikuttavat olevan ristiriidassa keskenään. Oletuksena yleensä on, että henkilötietojen suojan taso laskee, kun niiden siirtoa tehostetaan. Koska tietosuoja-asetus on kaikissa jäsenvaltioissa suoraan sovellettavaa oikeutta ja takaa siten yhtä hyvän suojan kaikkialla EU:ssa, henkilötietojen suojan ei kuitenkaan pitäisi laskea huolimatta tietojen siirron helpottamisesta sisämarkkinoilla. Mutta voidaanko henkilötiedoilla katsoa olevan vielä jonkinlaista suojaa, kun tarpeeksi moni taho on saanut ne haltuunsa? Vaikka henkilötiedot eivät läheskään aina ole salaisia, tilanne on periaatteessa verrannollinen siihen, ettei salaisuus ole enää salaisuus, kun tarpeeksi moni tietää sen.

Henkilötiedot leviävät useammalle taholle, kun niitä on helpompi siirtää. Mitä laajemmin tietoja siirretään, sitä vaikeampaa rekisteröidyn on kontrolloida tietojansa. Paremman kontrollin antaminen rekisteröidylle on tietosuoja-asetuksen lähtökohta,[239] mutta henkilötietojen vapaa liikkuvuus nakertaa rekisteröidyn kontrollointimahdollisuuksien tosiasiallista toteutumista. Rekisteröidyn ei ole mahdollista hallita tietojaan, mikäli hän ei tiedä, millä tahoilla on hänestä henkilötietoja. Usein henkilötietoja siirretään vielä eteenpäin kolmansil-

[237] Kuner 2012, s. 89.
[238] Bräutigam 2012, s. 417–418.
[239] TSA johdanto, kohta 7.

le osapuolille. Rekisteröidyn on siten lähes mahdotonta olla perillä siitä, minne kaikkialle hänen tietojansa on päätynyt, vaikka siirtoon pyydettäisiinkin lupa rekisteröidyltä ja kaikista vastaanottavista tahoista kerrottaisiin. Toisaalta henkilötiedoilla pitäisi olla kaikkialla sisämarkkinoilla korkeatasoinen suoja, joten vaikka rekisteröidyn kontrolli heikkenisikin, pitäisi suojan pysyä yhtä hyvänä kuin tilanteessa, jossa henkilötietoja ei voisi siirtää niin helposti, jolloin ne myös olisivat harvempien hallussa. Kun henkilötiedoille taataan korkeatasoinen suoja, saadaan helpommin epäilevämmänkin yksilön luottamus. Kuitenkin tosiasia on, että mitä useammalla taholla on hallussaan henkilötietoja, sitä suurempi on käytännössä tietosuojaloukkausten todennäköisyys sääntelystä ja hyvistä pyrkimyksistä huolimatta.

Henkilötietojen vapaa liikkuvuus helpottaa yritysten toimintaa sisämarkkinoilla huomattavasti, mutta tietosuoja-asetuksen sääntely henkilötietojen siirrosta tuo muutenkin etua EU:n alueelle sijoittautuneille yrityksille. Henkilötietojen siirto kolmansiin maihin on nimittäin kaikkea muuta kuin vapaata. Vaikka siirto kolmanteen maahan olisikin sallittua, tietojen säilyttäminen EU:ssa ja siten tietosuoja-asetuksen vaatimusten täyttäminen voi olla paljon yksinkertaisempaa. Tämä tuo markkinaetua esimerkiksi EU:ssa sijaitseville uusille pilvipalveluyrityksille.[240]

6.2. Henkilötietojen siirto EU:sta kolmansiin maihin

Tietosuoja-asetuksen tarkoituksena on helpottaa henkilötietojen siirtoa nimenomaan EU:n jäsenmaiden välillä, jolloin sen tuoma etu kohdistuu sisämarkkinoihin. Globalisaation myötä henkilötietoja on siirrettävä kuitenkin myös EU:n ulkopuolelle kolmansiin maihin, minkä vuoksi EU:n haasteena on turvata henkilötietojen suoja ”ilman minkäänlaisia porsaanreikiä”.[241] Mikäli siirretyt henkilötiedot olisivat EU:n tietosuojalainsäädännön ulottumattomissa, se aiheuttaisi selkeän uhan henkilötietojen suojalle, mikäli kolmannessa maassa ei ole yhtä kattavaa henkilötietojen suojaa kuin EU:ssa.

Vaikka henkilötiedot olisivat kolmannessa maassa saatavilla, se ei tarkoita, että kyseessä on henkilötietojen siirto. Lindqvist-tapauksessa EUT linjasi, että henkilötietojen laittaminen internetiin ei ollut henkilötietojen siirtoa kolmansiin maihin, vaikka toiminta samalla mahdollistikin pääsyn kyseisiin tietoihin.[242] Henkilötietojen siirto voi tapahtua monella eri

[240] https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain
[241] COM (2012) 9, s. 12.
[242] C-101/01, kohdat 67–70.

tavalla ja lopullinen määritelmä riippuu tapauskohtaisesta tilanteesta. Yleisenä suuntaviivana voidaan sanoa, että henkilötietojen siirto on kyseessä, kun tiedot vastaanotetaan kolmannessa maassa esimerkiksi rekisterinpitäjän toimipaikassa — pelkkä tietojen saatavilla olo internetissä ei sitä ole.[243] Henkilötietojen siirto ei ole kyseessä esimerkiksi Googlen näyttäessä hakutuloksia ympäri maailmaa. Sen sijaan silloin, kun Google siirtää tietoja EU:sta jollekin kolmannessa maassa sijaitsevalle palvelimelle, henkilötietojen siirto on tapahtunut.

6.2.1. Tietosuojan riittävä taso edellytyksenä henkilötietojen siirrolle

Toisin kuin EU:ssa tapahtuvassa henkilötietojen siirrossa, EU:sta kolmansiin maihin kohdistuvien siirtojen sääntelyssä keskiössä on siirron esteiden poistamisen sijaan luonnollisten henkilöiden henkilötietojen korkeatasoinen suoja. EU:n rajoituksien noudattaminen henkilötietojen siirrossa onkin yksi suurimmista haasteista, joita kansainvälisillä yrityksillä ja muilla organisaatioilla on toimiessaan EU:n alueella.[244] TSA 44 artiklasta, jossa säädetään yleisestä periaatteesta koskien henkilötietojen siirtoja kolmansiin maihin, ilmenee selkeästi EU:n tavoite lainsäädäntönsä ekstraterritoriaaliseen vaikutukseen. Kyseisen artiklan mukaan

> *”Sellaisten henkilötietojen siirto, joita käsitellään tai joita on tarkoitus käsitellä kolmanteen maahan tai kansainväliselle järjestölle siirtämisen jälkeen, toteutetaan vain jos rekisterinpitäjä ja henkilötietojen käsittelijä noudattavat tässä luvussa vahvistettuja edellytyksiä ja ellei tämän asetuksen muista säännöksistä muuta johdu; tämä koskee myös henkilötietojen siirtämistä edelleen kyseisestä kolmannesta maasta tai kansainvälisestä järjestöstä toiseen kolmanteen maahan tai toiselle kansainväliselle järjestölle. Kaikkia tämän luvun säännöksiä on sovellettava, jotta varmistetaan, että tällä asetuksella taattua luonnollisten henkilöiden henkilötietojen suojan tasoa ei vaaranneta”.*

Kääntäen sanottuna artikla kieltää henkilötietojen siirron kolmanteen maahan, ellei siellä noudateta EU:n vaatimuksia eli tietosuoja-asetuksen V luvun edellytyksiä henkilötietojen käsittelyssä. EU:n tietosuojanormit ovat monin paikoin tiukempia kuin muualla, mutta tarkoituksena ei ole kuitenkaan estää kokonaan henkilötietojen siirtoa EU:n ulkopuolelle. Päinvastoin EU pyrkii luomaan puitteet, joissa se voisi yhdistää laadukkaan ja korkean

[243] Kuner 2013, s. 13–14, ja Kuner 2012, s. 156.
[244] Ustaran 2018, kpl 12.9. (ei sivunumerointia)

tietosuojan tason ja samalla helpottaa tiedonsiirtoa rajojen yli kolmansiin maihin.[245] Tiedonsiirto rajojen ulkopuolelle on tärkeää, sillä liian tiukalla linjalla olisi negatiivisia vaikutuksia EU:n alueen yritysten toimintaan. Talouden nimissä henkilötietojen suojasta ollaan valmiita joustamaan jonkin verran.

Henkilötietojen siirto kolmanteen maahan on sallittua ensinnäkin silloin, kun komissio on TSA 45 artiklan mukaisesti todennut, että kohdemaa varmistaa ”riittävän tietosuojan tason”. Tällöin rajatylittävä henkilötietojen siirto on sallittua komission päätöksen perusteella eikä erillistä lupaa tarvita, mikä yksinkertaistaa henkilötietojen siirron ja vaaditun tietosuojan yhdistämistä. Komissio on katsonut riittävän henkilötietojen suojan täyttyvän esimerkiksi Argentiinassa, Sveitsissä, Israelissa ja Uudessa-Seelannissa.[246]

”Riittävä taso” osoittaa, että kolmannen maan takaaman suojan ei tarvitse olla yhtä korkea kuin EU:ssa, mutta sen on pääosiltaan vastattava EU:n vaatimuksia tietosuojasta niin, ettei tietosuojasäännösten kiertäminen olisi mahdollista henkilötietojen siirrolla.[247] Arvioitaessa tietosuojan riittävän tason täyttymistä huomioidaan kolmannen maan lainsäädäntö sekä se, kuinka kyseinen valtio kunnioittaa oikeusvaltioperiaatetta, ihmisoikeuksia ja perusvapauksia (TSA 45(2)). Käytännössä kolmannen maan käsityksen henkilötietojen suojasta tulisi siten vastata EU:ssa vallitsevaa. Myös yksityisyys ja sen merkitys tulisi niin ikään ymmärtää samankaltaisesti, sillä sen suojaaminen on asetuksen tavoitteena. Tätä kautta EU voi mahdollisesti vaikuttaa kyseisten oikeuksien perus- ja ihmisoikeusasemaan kolmannessa maassa sekä siihen, kuinka niitä tulkitaan varsinkin yksityisyyden ollessa hyvin kulttuurisidonnainen. Suurin osa rajatylittävistä henkilötietojen siirroista ei kuitenkaan perustu komission antamiin päätöksiin tietosuojan riittävästä tasosta,[248] joten mekanismin vaikutus henkilötietojen suojan ja yksityisyyden mahdolliseen parantumiseen kolmansissa maissa on käytännössä mitätön. Komission päätökset riittävästä tietosuojasta kohdistuvat vain kehittyneisiin maihin, jotka pitkälti jakavat samat näkemykset EU:n kanssa.

Päätöstä tehdessään komission on otettava huomioon kaikki henkilötietojen suojaan vaikuttavat olosuhteet kolmannessa maassa vallitsevan tietosuojan tosiasiallista tasoa arvioitaessa. Pelkkä lainsäädännön tarkasteleminen ei riitä, vaan myös sen noudattamiseen on

[245] COM (2012) 9, s. 11.
[246] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
[247] C-362/14, kohta 73 ja julkisasiamiehen ratkaisuehdotus C-362/14, kohta 141.
[248] Bräutigam 2016, s. 145.

kiinnitettävä huomiota.[249] Lisäksi komission tulee seurata kolmannessa maassa tapahtuvaa kehitystä ja väliajoin tarkastaa, ettei suojan taso ole laskenut vaaditusta, sekä mahdollisesti kumota aiempi päätös, jos henkilötietojen suoja ei enää ole riittävällä tasolla kyseisessä maassa (TSA 45(3–5) art.). Edeltävässä henkilötietodirektiivissä vaatimusta väliajoin tehtävistä tarkastuksista ei ollut, ja se on selkeästi seurausta Schrems-tapauksesta,[250] jota käsitellään tarkemmin myöhemmin.

Mikäli komission päätöstä ei ole koskien kolmatta maata, johon henkilötietoja ollaan siirtämässä, siirto on TSA 46 artiklan mukaan sallittua, jos rekisterinpitäjä on toteuttanut asianmukaiset suojatoimet ja jos rekisteröityjen turvana on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja. Asianmukaisia suojatoimia ovat muun muassa yritystä koskevat sitovat säännöt, komission hyväksymät vakiolausekkeet sekä tietosuojaviranomaisen vahvistamat ja komission hyväksymät käytännesäännöt. Tällöin kolmannessa maassa vallitsevalla tietosuojan tasolla ei ole merkitystä, kun yritys omassa toiminnassaan sitoutuu noudattamaan EU:n vaatimaa tietosuojan tasoa. Jos TSA 46 artiklan edellyttämiä suojatoimia ei ole toteutettu eikä komission päätöstä riittävästä tietosuojan tasosta myöskään ole, henkilötietojen siirto kolmanteen maahan on sallittua vain TSA 49 artiklan mukaisissa erityistilanteissa. Näitä ovat esimerkiksi rekisteröidyn itsensä antama suostumus henkilötietojensa siirtoon tai kun siirto on tarpeen tärkeän yleisen edun vuoksi, elintärkeiden etujen suojaamiseksi tai oikeusvaateen tekemiseksi. Rajatylittävien henkilötietojen siirto on tällöin huomattavasti hankalampaa ja rajatumpaa.

EU:n sääntely henkilötietojen siirrossa on selkeästi suoraan ekstraterritoriaalista, vaikka periaatteessa se kohdistuu sisämarkkinoihin. Se ensinnäkin vaikuttaa toimijoihin kolmansissa maissa suoraan, mikäli ne haluavat toimia sisämarkkinoilla tai tehdä yhteistyötä sisämarkkinoilla olevien kanssa ja siirtää henkilötietoja pois EU:sta. Sääntely vaikuttaa tätäkin laajemmalti, koska samat vaatimukset henkilötietojen riittävästä suojasta ja EU:n vaatimusten noudattamisesta asetetaan myös myöhemmille kolmansien maiden välillä tapahtuville henkilötietojen siiroille, kun henkilötieto on alun perin EU:sta (TSA 44 art.). EU ulottaa lainsäädäntönsä selvästi oman lainkäyttöpiirinsä ulkopuolelle, mikä on tarpeen, jotta tavoiteltu henkilötietojen suoja todella toteutuisi.

[249] C-362/14, kohta 75–76.
[250] Bräutigam 2016, s. 148.

Vaikka yhtä korkeatasoista suojaa ei vaaditakaan, EU vaikuttaa globaalisti rekisterinpitäjien toimintaan sääntelemällä henkilötietojen siirtoa riippumatta siitä, onko rekisterinpitäjällä itsellään suoraa yhteyttä EU:hun. Sääntelyn vaikutus voi olla Bryssel-efektin myötä vielä laajempi. Jotta Bryssel-efektin voidaan sanoa tulevan kyseeseen, täytyy EU:n tietosuojalainsäädännön vaikuttaa myös muiden henkilötietojen suojaan kuin vain EU:ssa oleskelevien. Kuten aiemmin todettiin, edellytykset Bryssel-efektin toteutumiselle täyttyvät EU:n ollessa tarpeeksi suuri markkinavoima, jolla on vahva lainsäädäntökapasiteetti ja kyky asettaa merkittäviä sanktioita. Lisäksi sääntelyn kohde eli henkilötiedot eivät voi karata toiseen lainkäyttöpiirin, sillä sääntely nimenomaan estää sen silloin, kun edellytykset siirrolle eivät täyty. Jos kolmannessa maassa henkilötietojen suoja on tietosuoja-asetuksen vaatimalla riittävällä tasolla ja siirto on komission päätöksen perusteella sallittua, mahdollisesta Bryssel-efektistä ei voida sanoa mitään, sillä kyseisellä valtiolla voi olla sama tavoite turvata henkilötietojen suoja ilman, että EU olisi siihen vaikuttanut. EU:n tietosuojasääntelyn ekstraterritoriaalista vaikutusta ei voida tällöin todeta, muttei kiistääkään.

Sen sijaan jos tietosuojan taso ei ole riittävä ja siirto sallitaan TSA 46 art. perusteella, tilanne on eri. Kun siirto on sallittua yritystä koskevien sitovien sääntöjen perusteella, Bryssel-efekti toteutuu tällöin tehokkaasti. Pohjimmiltaan yritystä sitovissa säännöissä kyse on monikansallisten yritysten itselleen laatimista globaaleista säännöistä ja ohjeista, jotka perustuvat EU:n asettamiin standardeihin yksityisyydestä ja henkilötiedoista.[251] Yrityksen ei ole mitenkään taloudellisesti kannattavaa ja tehokasta luoda EU:sta peräisin oleville henkilötiedoille omaa erillistä rekisteriään, toimintaohjeita ja käytänteitä. Yrityksen toiminnasta riippuen sen toteuttaminen voi olla mahdotontakin. Näin ollen on melko varmaa, että yritys noudattaa kaikessa henkilötietojen käsittelyssä EU:n vaatimuksia riippumatta henkilötietojen alkuperästä, jolloin myös kolmansissa maissa olevat rekisteröidyt pääsevät nauttimaan EU:n tietosuojalainsäädännön tuomasta suojasta. Samalla tavalla yritysten on järkevää noudattaa vain yhtä toimintamallia henkilötietojen käsittelyssä, kun niille on sallittu henkilötietojen siirto perustuen muihin TSA 46 artiklassa mainittuihin suojatoimiin, kuten sitoviin käytännesääntöihin tai sertifiointeihin. Tällöinkin Bryssel-efekti toimii.

Bryssel-efekti ei kuitenkaan toteudu, jos henkilötietojen siirto sallitaan erityistilanteessa TSA 49 artiklan mukaisesti. Esimerkiksi kun rekisteröity antaa suostumuksensa siirrolle puutteellisesta tietosuojan tasosta huolimatta, ei EU:n vaatimuksilla ole enää merkitystä,

[251] Ustaran 2018, kpl 12.7.1. (ei sivunumerointia).

kunhan suostumus on EU:n sääntelyn mukainen. Rekisteröidylle täytyy kertoa tietosuojaan liittyvistä riskeistä ennen suostumuksen antamista. Jos hän riskeistä huolimatta haluaa suostua siirtoon, mikään taho ei voi kieltää häntä antamasta suotumustaan. Siten henkilötietojen suojasta on mahdollista luopua sen perus- ja ihmisoikeusoikeusasemasta huolimatta toisin kuin esimerkiksi henkilökohtaisesta koskemattomuudesta, jossa loukatun suostumus ei ole pätevä. Samoin tämä on jälleen osoitus rekisteröidylle annetusta kontrollista. Suostumuksen voi myöhemmin peruuttaa, joten EU:n sääntely vaikuttaa kuitenkin taustalla edelleen. Rekisteröidyn omaan suostumukseen perustuvien siirtojen voitaisiin periaatteessa katsoa heikentävän tietosuoja-asetuksen ekstraterritoriaalista vaikutusta, mutta käytännössä sen merkitys on vähäinen. Yrityksen on todennäköisesti tehokkaampaa noudattaa EU:n sääntelyä kuin informoida jokaista rekisteröityä erikseen ja pyytää heiltä tietojen siirtoon suostumusta, jonka saaminen on riskeistä ilmoittamisen jälkeen huomattavasti epävarmempaa. Koska suostumuksen pitää olla nimenomainen, oma kysymyksensä on, voidaanko tällaisessa tilanteessa pitää hyväksyttävänä rasti-ruutuun tyylisiä suostumuslomakkeita, joita harva todellisuudessa lukee.

Henkilötietojen siirron sääntelyssä Bryssel-efekti toteutuu ainakin *de facto* yritysten kautta, mutta myös *de jure* vaikutus on havaittavissa. EU:n tietosuojasääntely on nimittäin ollut vaikuttamassa kolmansien maiden lainsäädäntöön, kuten Australiassa heidän uudistaessaan lainsäädäntöään yksityisyydestä.[252] Verrattuna esimerkiksi oikeuden tulla unohdetuksi ekstraterritoriaalisuuteen vaikutus on tässä kohtaa myös kokonaisvaltaisempi. Vaatimalla riittävää tietosuojan tasoa edellytyksenä henkilötietojen siirrolle EU vaikuttaa henkilötietojen suojaan kolmansissa maissa laajemmin, koska vaatimus kohdistuu suojaan kokonaisuudessaan eikä vain osaan siitä. Jos oikeudella tulla unohdetuksi olisi ekstraterritoriaalista vaikutusta, se tarkoittaisi vain, että kyseinen oikeus toteutuisi, muttei välttämättä vaikuttaisi henkilötietojen suojaan sen enempää.

Henkilötietojen siirrossa ekstraterritoriaalinen vaikutus toteutuu kolmansissa maissa tehokkaasti. Jos yritykset eivät halua sopeutua tiukempaan tietosuojasääntelyyn, niiden täytyy pysyä poissa EU:n sisämarkkinoilta, mikäli niiden toiminnassa käsitellään henkilötietoja, mitä nykyään oikeastaan kaikki yritykset tekevät. Samalla ne myös rajaavat itsensä EU:sta siirrettävien henkilötietojen vastaanottamis- ja käsittelymahdollisuuden ulkopuolelle. Pienille, paikallisille yrityksille tämä ei ole ongelma, mutta suurille yrityksille sillä on

[252] Lynskey 2015, s. 43.

merkitystä, sillä globaalissa kilpailussa niillä ei ole varaa menettää EU:n markkinoita tai EU:ssa toimivia yhteistyökumppaneita.

EU on siten tarpeeksi vahva vaikuttaakseen globaalisti. Mikäli EU olisi pienempi ja heikompi, voisi EU itse asiassa aiheuttaa itselleen haittaa tiukalla tietosuojalainsäädännöllä. Tällöin se vaikeuttaisi yritystensä toimintaa eikä kolmansien maiden yrityksillä olisi niin suurta intressiä tulla sisämarkkinoille ja noudattaa EU:n sääntelyä. Pelkästään kuitenkaan EU:n suuruudella ei ole merkitystä vaan myös vastapuolen, mikä on hyvin havaittavissa Yhdysvaltojen kohdalla. Se on itsekin tarpeeksi vahva ja merkittävä, jotta se voi usein toimia omalla hyväksi katsomallaan tavalla välittämättä muista. Niinpä EU ei ole voinut suoraan sanella, kuinka Yhdysvaltojen tulisi toimia. Vaikka EU:lla onkin ollut vaikutusta, sen on myös täytynyt kuunnella Yhdysvaltoja. Yhdysvalloilla on mahdollisuus aiheuttaa suurta taloudellista haittaa EU:lle niin halutessaan, aivan kuten EU voi tehdä Yhdysvalloille.

6.2.2. Kolmannen valtion suvereenius — tapaus Schrems

EU:n ja Yhdysvaltojen välillä on selkeä ero, kuinka yksityisyyteen suhtaudutaan, mikä heijastuu myös yhteisymmärryksen puuttumiseen henkilötietojen suojasta ja niiden käsittelystä. EU:n sääntely henkilötietojen suojasta on selvästi tiukempaa kuin Yhdysvalloissa, ja Yhdysvallat onkin yrittänyt estää EU:n tietosuojalainsäädännön vaikutuksia.[253] Silloisessa henkilötietodirektiivissä henkilötietojen siirto oli kielletty kolmansiin maihin samalla tavalla kuin tietosuoja-asetuksessa, mikäli henkilötietojen suoja ei ollut riittävää. EU:n mielestä näin oli Yhdysvaltojen kohdalla. Näkemyserot henkilötietojen suojasta aiheuttivat pidemmän aikaa taistelua EU:n ja Yhdysvaltojen välillä, ja kiista pyrittiin ratkaisemaan vuonna 2000 niin sanotulla Safe Harbour -sopimuksella (komission päätös 2000/520).[254]

Safe Harbour -sopimuksessa ja sen liitteissä määriteltiin henkilötietojen suojan periaatteet, joiden noudattamiseen sitoutumisella yritykset saivat luvan siirtää ja käsitellä EU:sta kerättyjä henkilötietoja (päätöksen 1 art.). Järjestelmä perustui yritysten omaan varmennukseen (päätöksen 2 ja 3 art.). Safe Harbourilla luotiin raamit toimintatavoille, joilla riittävä tietosuojan taso ja sitä kautta henkilötietojen siirto voitiin varmistaa, ja se oli erittäin tärkeä taloudellisen toiminnan jatkamiseksi ja turvaamiseksi Yhdysvaltojen ja EU:n välillä. Hen-

[253] Bradford 2012, s. 22–23.
[254] Whitman 2004, s. 1156.

kilötietojen siirto on olennainen osa Atlantin yli käytävää kauppaa,[255] joten tietojen siirron hankaloittamisella EU olisi aiheuttanut myös itselleen hallaa.

Sopimuksessa määritettyihin periaatteisiin sitoutuneista yrityksistä tuli siten kuvainnollisesti sopimuksen nimen mukaisesti ”turvasatamia” henkilötiedoille Yhdysvalloissa. Tai ainakin tämä oli EU:n tavoite. Kuitenkin vuonna 2013 Edward Snowdenin paljastukset Yhdysvaltojen tiedustelupalvelujen laajasti harjoittamasta vakoilusta ja tarkkailusta musersivat Safe Harbourin merkityksen. Snowdenin paljastusten myötä ilmeni, että esimerkiksi NSA (National Security Agency) kerää yksityishenkilöistä tietoja ilman, että heitä epäiltäisiin mistään rikoksesta.[256] Samoin paljastui salainen PRISM-ohjelma, jossa oli mukana mm. Microsoft, Apple, Google, Yahoo, YouTube, Skype ja Facebook. Ne antoivat NSA:lle pääsyn käyttäjiensä tietoihin, viesteihin, hakuihin ja kuviin.[257] Kaikki edellä mainitut yritykset osallistuivat Safe Harbour -järjestelmään, jonka turvin ne saivat siirtää henkilötietoja EU:sta Yhdysvaltoihin. Siten samalla myös NSA pääsi siirrettyihin henkilötietoihin käsiksi, joten Safe Harbour -sopimuksen yhdysvaltalainen tulkinta käytännössä mahdollisti tiedusteluviranomaisten vakoilun EU:sta peräisin oleviin tietoihin.[258]

Paljastusten seurauksena syntyi suuria epäluuloja niin henkilötietojen käsittelystä Yhdysvalloissa kuin myös yhdysvaltalaisista teknologiayrityksistä. Esimerkiksi kaikkien EU:ssa asuvien Facebook-palvelun käyttäjien henkilötiedot siirrettiin Yhdysvaltoihin käsiteltäväksi. Tämän takia Maximillian Schrems teki Irlannin tietosuojavaltuutetulle kantelun, jotta tämä kieltäisi Facebookia siirtämästä Schremsin henkilötietoja Yhdysvaltoihin. Hänen mukaansa henkilötiedoilla ei ollut riittävää suojaa Yhdysvalloissa eikä niitä siten olisi saanut siirtää Yhdysvaltoihin. Tietosuojavaltuutettu kuitenkin hylkäsi Schremsin kantelun, sillä Yhdysvaltain tiedustelupalvelujen pääsystä käsiksi hänen tietoihinsa ei ollut näyttöä ja Facebook oli sitoutunut Safe Harbour -päätöksen periaatteisiin, jolloin riittävän tietosuojan taso oli komission päätöksellä taattu, eikä siirron kieltämiselle ollut perusteita.[259]

Niinpä Schrems vei asiansa High Courtiin, joka katsoi yhdysvaltalaisten tiedustelupalvelujen toiminnan olevan vastoin suhteellisuusperiaatetta tarkkailun ja tietojen kaappaamisen

[255] COM (2013) 846, s. 2.
[256] Ks. esim. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order ja https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?noredirect=on&utm_term=.0a970386ca93
[257] https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[258] COM (2013) 847, s. 17.
[259] C-362/14, kohdat 27–29.

ollessa aivan liian laajoja ja perusteettomia. Irlannin lainsäädännön mukaan tietosuojavaltuutetun olisi tullut tutkia kantelu, mutta koska asiassa sovellettiin EU:n oikeutta, High Court teki ennakkoratkaisukysymyksensä siitä, voiko tietosuojavaltuutettu riittävän tietosuojan takaavasta Safe Harbour -päätöksestä huolimatta tutkia kantelun.[260] Periaatteessa tapauksen pääasia koski siten tietosuojavaltuutetun toimivaltaa, joka EUT:n mukaan ulottui kanteluiden tutkimiseen myös tilanteissa, joissa komissio on antanut päätöksen kolmannen maan tietosuojan riittävästä tasosta.[261] Tosiasiallisesti Schrems oli myös asettanut Safe Harbour -päätöksen riidanalaiseksi, joten EUT tutki päätöksessään sen pätevyyden.[262]

Snowdenin paljastusten tultua ilmi komissio oli katsonut jo ennen Schrems-tapausta, että Safe Harbour -järjestelmän soveltamista ei voida enää jatkaa samaan tapaan ja se aloitti neuvottelut Yhdysvaltojen kanssa. Se ei kuitenkaan kumonnut päätöstään, koska se olisi aiheuttanut merkittävää taloudellista haittaa sekä EU:ssa olevien että yhdysvaltalaisten yritysten toiminnalle.[263] Komissio painotti siten taloutta ja kansainvälistä kauppaa enemmän kuin perusoikeuksien eli yksityisyyden ja henkilötietojen suojan mahdollisimman täysimääräisen toteutumista.

Sen sijaan EUT otti toisen linjan. Ratkaisussaan se julisti Safe Harbour -sopimuksen pätemättömäksi heti ilman siirtymäaikaa, mikä tuli yllätyksenä sekä komissiolle että yrityksille.[264] EUT katsoi, että sopimuksen 1 artikla oli pätemätön, koska Yhdysvaltain kansalliselle turvallisuudelle, yleiselle edulle ja lainsäädännön vaatimuksille annettiin päätöksessä etusija, joka syrjäytti Safe Harbour -sopimuksen periaatteet rajoituksetta. Tämä mahdollisti aivan liian laajan perusoikeuksiin puuttumisen ja loukkasi siten POK 7 ja 8 artikloja. Perusoikeuksista poikkeaminen olisi sallittua vain siinä laajuudessa kuin on ehdottoman tarpeen, miten Yhdysvallat ei toiminut. Rekisteröidyllä ei myöskään ollut mitään oikeussuojakeinoja tällaisia toimia vastaan.[265] Sopimuksen liitteiden mukaan periaatteiden noudattamista voitiin rajoittaa, mikäli lakisääteinen velvoite oli ristiriidassa Safe Harbour -periaatteiden kanssa, jolloin periaatteisiin sitoutuneen yrityksen tai muun organisaation tuli noudattaa Yhdysvaltain lakia ohi kyseisen sopimuksen. [266] Juuri tämä mahdollisti tiedustelupalvelujen laajan tietojensaannin Safe Harbourista huolimatta — tai pikemminkin sen avulla. Riippu-

[260] C-362/14, kohdat 30–36.
[261] C-362/14, kohdat 36–37, 66.
[262] C-362/14, kohta 67.
[263] COM (2013) 846, s. 8.
[264] Bräutigam 2016, s. 155.
[265] C-362/14, kohdat 84–86 ja 88–94.
[266] Päätöksen 2000/250 IV liitteen B kohta, EYVL L 215, s. 35.

matta Safe Harbour -periaatteiden varsinaisesta sisällöstä, sopimuksen 1 artikla ei täyttänyt HTD 25(6) artiklan perusoikeusnäkökulmasta tulkittavia vaatimuksia, joten se oli pätemätön.[267]

Myös sopimuksen 3 artikla katsottiin pätemättömäksi, sillä se esti kansallisia valvontaviranomaisia käyttämästä HTD 28 artiklan heille tuomia valtuuksia, joten komissio oli samalla päätöksessä ylittänyt oman toimivaltansa.[268] Koska artiklat 1 ja 3 olivat erottamaton osa päätöstä ja sen liitteitä, koko päätös katsottiin pätemättömäksi.[269] Kun mitään siirtymisaikaa ei annettu, komissiolle tuli kiire saada neuvottelut loppuun uudesta henkilötietojen siirtosopimuksesta Yhdysvaltain kanssa. Safe Harbour korvattiin Privacy Shield -sopimuksella (komission täytäntöönpanopäätös 2016/1250), joka oli edeltäjäänsä yksityiskohtaisempi ja asetti rekisterinpitäjän tiukempaan vastuuseen tietosuojasääntelyn noudattamatta jättämisestä.[270] Yksityiskohtaisemman sääntelyn lisäksi Privacy Shield -sopimuksen uusia elementtejä olivat muun muassa komission jatkuva seuraaminen tietosuojan riittävästä tasosta Yhdysvalloissa sekä riippumattoman, tietosuojasta vastaavan oikeusasiamiehen viran perustaminen,[271] jonka tarkoitus on toimia rekisteröidyille oikeussuojakeinona, jonka puutetta EUT peräänkuulutti Schrems-tuomiossa.

Uudistuksista huolimatta Privacy Shield on kohdannut kritiikkiä. Toisaalla katsotaan, ettei uusi sopimus muuta mitään Yhdysvaltojen jatkaessa edelleen tiedustelutoimintaansa, toisaalla taas yhdysvaltalaiset yritykset pitävät uutta sopimusta liian rasittavana ja kalliina noudattaa.[272] Järjestelmän noudattamista voidaan rajoittaa kansallisen turvallisuuden, julkisen edun tai lainvalvonnan vaatimusten perusteella. Edelleen rajoittaminen on mahdollista, jos laista, hallituksen asetuksista tai tuomioistuimien päätöksistä seuraa järjestelmän kanssa ristiriidassa olevia velvoitteita.[273] Näin ollen herää kysymys, ovatko uudistukset ja ero Safe Harbour -päätökseen tosiasiassa todellisia. Toisaalta myös sekä nykyisestä tietosuoja-asetuksesta että entisestä henkilötietodirektiivistä voidaan poiketa esimerkiksi kansallisen turvallisuuden tai yleisen edun perusteella, joten järjestelmän mahdollinen rajoittaminen ei itsessään ole ongelma. Ongelma sen sijaan on se, että vaikka Privacy Shield -päätöksessä järjestelmän rajoittamisen sanotaan olevan mahdollista vain siinä määrin kuin sille on tar-

[267] C-362/14, kohta 98.
[268] C-362/14, kohdat 102 ja 104.
[269] C-362/14, kohdat 105–106.
[270] Bräutigam 2016, s. 158.
[271] Privacy Shield -sopimuksen 4 art. ja johdannon kohdat 65 ja 116.
[272] Bräutigam 2016, s. 164–165.
[273] Privacy Shield -sopimuksen II liitteen I.5 kohta, EUVL L 207, s. 49.

vetta, tarpeellisuuden vaatimus on joustava ja se voidaan ymmärtää hyvin eri lailla. Koska asenne yksityisyyttä ja henkilötietojen suojaa kohtaan on Yhdysvalloissa erilainen kuin EU:ssa, epäilykset Yhdysvaltojen tiedustelupalvelun toimintatapojen muuttamisesta ovat perusteltuja, koska järjestelmästä poikkeamista voidaan tulkita edelleen samoin kuin Safe Harbour -sopimuksen aikaan. Tällöin Yhdysvaltojen tiedustelupalvelut voivat jatkaa toimintaansa entiseen tapaansa.

Tietosuojavaltuutettujen työryhmän mukaan Yhdysvaltain tiedustelupalveluiden tietojenkeruu ja niiden laajuus herättivät edelleen kysymyksiä, minkä vuoksi nimenomaan toimien tarpeellisuuden ja oikeasuhtaisuuden määritelmä tulisi tarkistaa ja selventää sekä varmistaa tarkkailuohjelmien valvonta. Lisäksi työryhmän arvion mukaan esimerkiksi periaatteista tulisi antaa selvemmät ohjeet, yksilöiden tiedottaminen heidän oikeuksistaan ja oikeussuojakeinoistaan pitäisi varmistaa paremmin kuin myös parantaa Privacy Shield -periaatteiden valvontaa. Myöskään asiamiestä ei pidetty tarpeeksi vahvana ja itsenäisenä, jotta sitä voitaisiin pitää tehokkaana oikeussuojakeinona.[274] Vaikka Privacy Shieldin myötä kehitystä on tapahtunut henkilötietojen suojassa niiden siirrossa Yhdysvaltoihin, järjestelmässä on edelleen useita ongelmallisia kohtia. Mikäli tilanteessa ei tapahdu muutosta ja toimenpiteisiin ei ryhdytä, tietosuojavaltuutetut aikovat itse ryhtyä tarpeellisiin toimiin viemällä asian kansallisiin tuomioistuimiin ja sitä kautta asettaa Privacy Shield -sopimuksen pätevyyden EUT:lle arvioitavaksi.[275] Tietosuoja-aktivistien huoli Privacy Shieldin paremmuudesta on siten aiheellinen.

Vaikka uusi sopimus onkin parannusta edelliseen, se ei edelleenkään toimi niin hyvin kuin EU:n tavoitteena ja tarkoituksena on. Safe Harbour ja Privacy Shield osoittavat hyvin neuvottelujen ja sopimusten tekemisen hankaluuden verrattuna Bryssel-efektin kautta tapahtuvaan vaikuttamiseen. Samoin ne ovat osoitus, että EU ei voi käyttää painostusta kovin tehokkaasti Yhdysvaltoja vastaan, koska Yhdysvallat on myös hyvin vahva osapuoli. Vaikka EU voisi olla painokkaampi ja yrittää voimakkaammin vaikuttaa Yhdysvaltoihin mahdollisella taloudellisella haitalla estämällä henkilötietojen siirron, on hyvin selvää, että EU aiheuttaisi samalla haittaa myös itselleen. Pienempien kolmansien maiden ollessa vastapuolena tätä vaaraa ei ole. Yhdysvaltojen halu turvata oma suvereenius ilmenee Safe Harbour -sopimuksen liitteistä hyvin selvästi: ”vaikka Safe harbor -periaatteiden tarkoituksena on tasoittaa yksityisyyden suojassa Yhdysvaltojen ja Euroopan välillä esiintyviä eroja, Yh-

[274] WP 255, s. 8–10, 15–16 ja 19.
[275] WP 255, s. 4 ja 20.

dysvaltojen on kunnioitettava vaaleilla valittujen lainsäätäjien valtaoikeuksia”.[276] Tämä osoittaa hyvin, kuinka haluton Yhdysvallat on ollut noudattamaan EU:n tietosuojalainsäädännöstä seuraavia toimintatapoja tai edes tosiasiallisesti pyrkimään yhteisymmärrykseen. Ymmärrettävästi se on pyrkinyt takaamaan oman lainkäyttövaltansa niin pitkälle kuin mahdollista.

Mikäli Privacy Shield -sopimusta ei olisi, Bryssel-efektin toteutuminen olisi epätodennäköistä Yhdysvaltojen kohdalla. Vaikka EU:lla on suuret markkinat ja yhdysvaltalaisilla yrityksillä on intressiä toimia niillä, EU:n yritykset ovat myös riippuvaisia yhdysvaltalaisista yrityksistä, etenkin teknologiajäteistä ja niiden palveluista. Sen seurauksena niiden yhteistyö EU:ssa olevien yritysten kanssa tulee turvata, koska muutoin EU:n yrityksille aiheutuisi suurta haittaa. Toisaalta vaikka EU:n vaikutusvalta Yhdysvaltojen suhteen ei ole sääntöjen sanelua, kuten joidenkin muiden kolmansien maiden kohdalla helpommin voi olla, EU:lla on vaikutusta myös yhdysvaltalaisten yritysten toimintaan. Valtakamppailua silti käydään EU:n ja Yhdysvaltojen välillä siitä, milloin yhteisistä tietosuojasäännöistä poikkeamiselle on perusteita ja milloin ei — kiista, jossa osapuolilla on edelleen hyvin erilaiset näkemykset yksityisyyden ja henkilötietojen suojan suhteesta turvallisuuteen ja yleiseen etuun.

[276] Päätöksen 2000/250 IV liitteen B kohta, EYVL L 215, s. 35.

7. Loppupäätelmät

Henkilötietojen suojaa ja oikeutta yksityisyyteen voidaan pitää maailmanlaajuisesti ihmisoikeutena, mutta yksityisyyden kulttuurisidonnaisuudesta johtuen näille oikeuksille annettava painoarvo ei ole muualla välttämättä niin vahva kuin EU:ssa. Vaikka henkilötietojen suoja ja yksityisyys usein vetävät eri suuntaan kuin sananvapaus, henkilötietojen keräämisellä ja yksityisyyden piiriin kajoamisella voidaan myös estää vapaa mielipiteiden muodostaminen ja ilmaiseminen, jotka ovat tärkeitä demokratian edistymiselle ja turvaamiselle. Tämä on todennäköisesti kulttuurin ohella toinen syy, miksi henkilötietojen suojalle ei anneta yhtä suurta painoarvoa kaikkialla. Kolmas syy on turvallisuuden painottaminen yksityisyyden ja henkilötietojen suojan kustannuksella.

EU:n omiin periaatteisiin kuuluu edistää ihmisoikeuksien, kuten henkilötietojen suojan, toteutuminen myös omien rajojensa ulkopuolella, mikä on yksi peruste ulottaa lainsäädäntöä omaa aluettaan laajemmalle. Lisäksi internetistä ja globalisaatiosta johtuen EU:n täytyy pyrkiä suojaamaan omalla alueellaan olevien ihmisten henkilötietoja laajemmin kuin vain omaan alueeseensa keskittyen. Henkilötietojen taloudellisesta merkityksestä johtuen niitä käsitellään lähtökohtaisesti kaikkien yritysten toiminnassa, mikä niin ikään lisää EU:n tarvetta vaikuttaa rajojensa ulkopuolella. Muutoin muualla vallitseva heikompi henkilötietojen suoja heikentää myös EU:ssa olevien henkilötietojen suojaa. EU:lla on erilaisia keinoja, joilla se voi vaikuttaa kansainvälisesti. Ensinnäkin se voi neuvotella ja muuten poliittisesti pyrkiä vaikuttamaan, mutta se ei aina ole kovin tehokasta. EU:n sääntelyn edistäminen kolmansissa maissa pelkästään perus- ja ihmisoikeuslähtökohdista on hankalaa, kuten oikeuden tulla unohdetuksi kohdalla havaitaan. Siinä EU:n joko täytyy myöntyä määräämään hakukoneiden toiminnasta vain omien rajojensa sisällä tai yrittää arvovallallaan tai mahdollisella painostuksellaan saada muu maailma hyväksymään oman sääntelynsä vaikutukset myös EU:n ulkopuolella.

Toinen tapa vaikuttaa kolmansissa maissa on markkinatalouden toiminnan kautta, mikäli Bryssel-efekti toteutuu. Tämän vaikuttamiskeinon heikkous on sen riippuvuus yritysten tosiasiallisesta toiminnasta, mihin ei ulkopuolelta voida vaikuttaa. Koska yritykset kuitenkin lähtökohtaisesti toimivat taloudellisesti tehokkaasti ja järkevästi turvatakseen toimintansa myös jatkossa, Bryssel-efektin toteutumista voidaan arvioida melko hyvin jo ennakkoon. Vaikka oikeuden tulla unohdetuksi kohdalla se ei toteudukaan, efektillä on yleisesti henkilötietojen suojaan liittyen vahvat mahdollisuudet toteutua. Henkilötietojen siirron

kohdalla Bryssel-efekti toteutuukin tehokkaasti, mitä kautta EU:n tietosuojalainsäädännöllä on selkeästi vaikutusta kolmansissa maissa.

Kolmas ja hienovaraisin keino vaikuttaa on ohjata ihmisten käyttäytymistä tiettyyn suuntaan. Kolmansien maiden ihmiset pitäisi kuitenkin saada EU:n tai EU:n arvoja edistävän toimijan piiriin niin, että käyttäytymiseen olisi edes mahdollista yrittää vaikuttaa. Tässäkin keinossa vaikuttaminen voi onnistua suuryritysten kautta, jotka ovat kuluttajien muuttuneen käyttäytymisen myötä muuttaneet omaa tarjontaansa ja siten vaikuttavat muidenkin kuluttajien toimintaan laajemmin. Lisäksi henkilötietojen suojan asemaa voidaan parantaa vaikuttamalla kolmannessa maassa vallitsevaan asenneilmapiiriin henkilötietoihin liittyen, mutta tällainen vaikutus voi olla hyvin hidasta ja vaatia pitkäjänteistä ohjaamista.

Voidaan perustellusti sanoa, että EU:lla on vaikutusvaltaa globaalisti koskien henkilötietojen suojaa. Vaikuttaessaan ekstraterritoriaalisesti EU:n toimintaa kritisoidaan imperialistiseksi. Täysin suora ekstraterritoriaalinen sääntely onkin usein kyseenalaista, koska silloin tunkeudutaan toisen valtion suvereniteetin piiriin. Varsinkin jos käsitys oikeuden tai velvollisuuden sisällöstä on hyvin erilainen, on varmaa, että EU:n omavaltaista sääntelyä vastustetaan. Vaikka yksityisyydellä ei Euroopan ulkopuolisissa kulttuureissa olisikaan niin suurta merkitystä, — mikä myös suoraan vaikuttaa siihen, ettei henkilötietojen suojaa välttämättä nähdä niin tärkeänä ihmisoikeutena — EU:n ekstraterritoriaalinen tietosuojasääntely on mielestäni oikeutettua, jos se edistää ja kehittää henkilötietojen suojaa kolmansissa maissa. Henkilötietojen suojalla on nimittäin ympäri maailmaa käytännössä kuitenkin sama merkitys ihmisille kuin Euroopassa, sillä uhat digitaalisessa ympäristössä ovat globaalisti samoja kaikkialla.

Kuten on tullut ilmi, internetin rajattomuuden ja maailmanlaajuisten yritysten myötä eri normistot törmäävät toisiinsa, ja niiden yhteensovittaminen on mahdotonta, jos toisaalla suojaa vaaditaan ja toisaalla sitä ei anneta. Sillä on suuri merkitys, kenen sääntöjä henkilötietojen käsittelyyn ja keräämiseen käytetään. Vaikka EU:ta kritisoidaan suvereenien valtioiden alueelle tunkeutumisesta, tosiasia on, että jos EU ei niin tee, joutuu EU puolestaan mukautumaan muiden käsityksiin henkilötietojen suojasta. Ainakin Yhdysvalloilla olisi huomattavasti enemmän vaikutusta henkilötietojen suojaan tai pikemminkin sen puuttumiseen, jos EU pysyisi vain omalla alueellaan. Tällöin suoja myös EU:ssa väistämättä heikkenisi.

Bryssel-efekti on hyvin tehokas keino vaikuttaa aiheuttamatta kysymyksiä kolmansien maiden suvereeniudesta. Henkilötietojen taloudellisen merkityksen seurauksena EU voi toimia henkilötietojen suojan kohdalla huomaamatta ihmisoikeuslähettiläänä Bryssel-efektin avulla. Taloudellisten syiden perusteella EU:n toimintaa voidaan myös kyseenalaistaa. Muualta tulevien yritysten pyrkiessä mukautumaan tiukempaan sääntelyyn EU:n yritykset saavat kilpailuetua, sillä niiden toiminta on jo lainsäädännön kanssa yhdenmukaista, minkä lisäksi niiden keskinäinen henkilötietojen siirto on huomattavasti helpompaa. Toisaalta EU:n yritykset ovat jo aiemmin joutuneet tekemään samat investoinnit henkilötietojen suojaan, joten sinänsä kenellekään ei ole annettu mitään helpotuksia. Taloudellisten seikkojen takia EU on itse asiassa hieman antanut periksi korkeatasoisesta suojasta. Koska henkilötietojen siirrossa kolmansiin maihin vaaditaan vain riittävää suojan tasoa, edellytykset eivät ole niin korkealla kuin EU:ssa. EU aiheuttaisi itselleen taloudellista haittaa, jos se tekisi henkilötietojen siirrot kolmansiin maihin liian vaikeaksi. Näin ollen tasapainoilu on välttämätöntä: Vaatimukset henkilötietojen suojasta tulee asettaa tarpeeksi korkealle, jotta se perus- ja ihmisoikeutena ei vaarantuisi tai heikkenisi. Kuitenkaan liian korkeatasoista suojaa ei voida vaatia, jotta EU:ssa olevat yritykset eivät joutuisi ahdinkoon.

Vaikka sekä henkilötietodirektiivin että tietosuoja-asetuksen toisena tavoitteena on sisämarkkinoiden integraation syventäminen, henkilötietojen suojan perusoikeusasema on normeissa vahvasti esillä ja vaikuttamassa niihin. Myös EUT:n ratkaisuissa tämä on nähtävissä, ja huomattakoon erityisesti Schrems-tapauksessa tehty päätös Safe Harbour -sopimuksen pätemättömyydestä. Ilman puitesopimusta henkilötietojen siirto on Yhdysvaltoihin huomattavasti hankalampaa, mikä aiheuttaa myös EU:ssa oleville yrityksille haittaa. Koska EUT julisti päätöksen pätemättömäksi vieläpä ilman siirtymäaikaa, edellä esitetyistä epäilyistä huolimatta voidaan katsoa, että henkilötietojen suoja perusoikeutena on asetettu korkeammalle ennen henkilötietojen huomattavaa merkitystä elinkeinoelämälle. Nämä molemmat näkökulmat kuitenkin luonnollisesti vaikuttavat sääntelyn taustalla.

Monet valtiot ovat ottaneet mallia EU:n sääntelystä, minkä perusteella sitä voidaan pitää onnistuneena siitä riippumatta, onko EU:n alkuperäisenä tavoitteena ollut vaikuttaa kolmansiin maihin vai ei. Ja mitä useampi valtio seuraa EU:n esimerkkiä, sitä suurempi paine syntyy muille valtioille seurata muutoksessa mukana. Vaikka EU ei aina voisikaan suoraan vaikuttaa ekstraterritoriaalisesti, sen asema on muutoksen alulle panijanakin näin ollen vahva.

Lähteet

Virallisaineisto

COM (2007) 581

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Interest: Succeeding in the age of globalisation. COM (2007) 581 final. 3.10.2007.

COM (2012) 9

Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle. Yksityisyydensuoja verkottuvassa maailmassa. Euroopan uusi tietosuojakehys. COM (2012) 9 final. 25.1.2012

COM (2013) 846

Komission tiedonanto Euroopan parlamentille ja neuvostolle. Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon. COM (2013) 846 final. 27.11.2013.

COM (2013) 847

Komission tiedonanto Euroopan parlamentille ja neuvostolle safe Harbour -järjestelmän toiminnasta EU:n kansalaisten ja EU:hun sijoittautuneiden yritysten näkökulmasta. COM (2013) 847 final. 27.11.2013.

COM (2017) 10

Ehdotus. Euroopan parlamentin ja neuvoston asetus yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus). COM (2017) 10 final. 10.1.2017.

EUVL C 347

Euroopan unionin virallinen lehti C 347, 16.10.2017, 60. vuosikerta.

EUVL L 207

Euroopan unionin virallinen lehti L 207/1. 1.8.2016. 59. vuosikerta

EYVL L 215

Euroopan yhteisöjen virallinen lehti L 215, 25.8.2000, 43. vuosikerta.

HE 9/2018 vp

Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.

Julkisasiamiehen ratkaisuehdotus C-131/12

Julkisasiamiehen ratkaisuehdotus, Niilo Jääskinen, Asia C-131/12 Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González, 25.6.2013.

Julkisasiamiehen ratkaisuehdotus C-362/14

Julkisasiamiehen ratkaisuehdotus, Yves Bot, Asia C-362/14 Maximillian Schrems vastaan Data Protection Commissioner, 23.9.2015.

KOM (2005) 525

Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle. Eurooppalaiset arvot globaalistuvassa maailmassa. KOM (2005) 525 lopullinen. 20.10.2005.

OMML 35/2017

EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö. Mietintöjä ja lausuntoja 35/2017, Oikeusministeriö.

WP 148, 1/2008

Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines, 00737/EN WP 148.

WP 169, 1/2010

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN WP 169.

WP 179, 8/2010

Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, 0836-02/10/EN WP 179.

WP 225

Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgement on “Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12, 14/EN WP 225.

WP 255

Article 29 Data Protection Working Party, EU – U.S. Privacy Shield – First annual Joint Review, 17/EN WP 255.

YK, A/HRC/27/37

The Right to Privacy in the Digital Age. Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, 30.6.2014.

YK 68/167

Resolution adopted by the General Assembly on 18 December 2013. Sixty-eighth session, agenda item 69 (b), A/RES/68/167.

Kirjallisuus

Aarnio 1997

Aarnio, Aulis: Oikeussäännösten systematisointi ja tulkinta, teoksessa Minun metodini (toim. Juha Häyhä). Helsinki 1997.

Acquisti 2009

Acquisti, Alessandro: Nudging Privacy. Behavioural Economics of Personal Information. IEEE Security & Privacy Vol. 7, Is. 6, 2009, s. 82–85.

Ali 2000

Ali, Shaheen Sardar: Gender and Human Rights in Islam and International Law. Equal Before Allah, Unequal Before Man? The Hague 2000.

Allen 1999

Allen, Anita L.: Coercing privacy. William and Mary Law Review, 1999, Vol. 40, s. 723–757.

Bach – Newman 2007

Bach, David – Newman, Abraham L.: The European regulatory state and global public policy: micro-institutions, macro-influence. Journal of European Public Policy, 2007, Vol. 14, No. 6, s. 827–846.

Barclay 2013

Barclay, Courtney A.: A comparison of proposed legislative data privacy protections in the United States. Computer Law & Security review, 2013, Vol. 29, s. 359–367.

Blume 2002

Blume, Peter: Protection of Informational Privacy. Copenhagen 2002.

Bradford 2012

Bradford, Anu: The Brussels Effect. Northwestern University Law Review, 2012, Vol. 107, No. 1, s. 1–68.

Bräutigam 2012

Bräutigam, Tobias: Getting High on Information? The European Commission's Proposal for Renewal of the Data Protection Legislation. JFT 5/2012, s. 415–435.

Bräutigam 2016

Bräutigam, Tobias: The land of confusion: international data transfers between Schrems and the GDPR, teoksessa Data protection, privacy and European regulation in the digital age (ed. Tobias Bräutigam and Samuli Miettinen). Helsinki 2016.

Bygrave 2001

Bygrave, Lee A.: The Place of Privacy in Data Protection Law. UNSW Law Journal, 2001, Vol. 24, No. 1, s. 277–283.

Cate 1998

Cate, Fred H.: The European Data Protection Directive and European–U.S. Trade. Currents: International Trade Law Journal, 1998, Is. 1, s. 61–80.

Choi et al. 2018

Choi, Hanbyul – Park, Jonghwa – Jung, Yoonhyuk: The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 2018, Vol. 81, s. 42–51.

Codagnone et al. 2014

Codagnone, Christiano – Bogliacino, Francesco – Veltri, Giuseppe A. – Lupiáñez-Villanueva, Francisco – Gaskell, George: Nudging in the World of International Policy Making, teoksessa The Behavioral Economics Guide 2014 (ed. Alain Samson), s. 51-58. https://www.behavioraleconomics.com/BEGuide2014.pdf

Cormack 2016

Cormack, Andrew: Is the subject access right now too great a threat to privacy? European Data Protection Law Review, 2016, Vol. 2, Is. 1, s. 15–27.

De Hert – Gutwirth 2009

De Hert, Paul – Gutwirth, Serge: Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action, teoksessa Reinventing data protection? (ed. Serge Gurthwirth, Yves Poullet, Paul De Hert, Cecile de Terwagne ja Sjaak Nouwt), Berlin 2009.

Ek 2014

Ek, Pia: Ikimuistoinen legenda vai menneisyyden vanki — onko urheilijalla oikeus tulla unohdetuksi? Urheilu ja oikeus, 2014, s. 114–122.

Forde 2016

Forde, Aidan: The Conceptual Relationship between Privacy and Data Protection. Cambridge Law Review, 2016, Vol. 1, s. 135–149.

Garrie – Byhovsky 2017

Garrie, Daniel – Byhovsky, Irene: Privacy and Data Protection in Russia. Journal of Law & Cyber Warfare, 2017, Vol. 5, Is. 2, 235–253.

Gellert – Gutwirth 2013

Gellert, Raphaël – Gutwirth, Serge: The legal constitution of privacy and data protection. Computer Law & Security Review, 2013, Vol. 29, s. 522–530.

Halpern 2015

Halpern, David: Inside teh Nudge Unit. How Small Changes Can Have a Big Difference. London 2015.

Herlin-Karnell 2012

Herlin-Karnell, Ester: The EU as a Promoter of Values and the European Global Project. German Law Journal, 2012, Vol. 13, No. 11, s. 1225–1246.

Hijmans 2016

Hijmans, Hielke: The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU. Berlin 2016.

Himma 2007

Himma, Kenneth Einar: Privacy Versus Security: Why Privacy is Not an Absolute Value or Right. San Diego Law Review, 2007, Vol. 44, s. 857–920.

Hirvonen 2011

Hirvonen, Ari: Mitkä metodit? Opas oikeustieteen metodologiaan. https://www.helsinki.fi/sites/default/files/atoms/files/hirvonen_mitka_metodit.pdf

Inness 1992

Inness, Julie C.: Privacy, Intimacy, and Isolation. New York 1992.

Jones 2014

Jones, Joseph: Control-alter-delete: the “right to be forgotten”. European Intellectual Property Review, 2014, Vol. 36, Is. 9, s. 595–601.

Kahneman 2011

Kahneman, Daniel: Thinking Fast and Slow. New York 2011.

Koillinen 2013

Koillinen, Mikael: Henkilötietojen suoja itsenäisenä perusoikeutena. Oikeus, 2/2013, s. 171–193.

Kulk — Zuiderveen Borgesius 2014

Kulk, Stefan — Zuiderveen Borgesius, Frederik: Google Spain v. González: Did the Court Forget about Freedom of Expression? European Journal of Risk Regulation, 2014, Is. 3, s. 389–398.

Kuner 2012

Kuner, Christopher: European Data Protection Law. Corporate Compliance and Regulation. 2nd edition. Oxford 2007, reprinted 2012.

Kuner 2013

Kuner, Christopher: Transborder Data Flows and Data Privacy Law. Oxford 2013.

Kuner 2015

Kuner, Christopher: The Court of Justice of the EU Judgement on Data Protection and Internet Search Engines. LSE Law, Society and Economy Working Papers 3/2015.

Kwamwangamalu 1999

Kwamwangamalu, Nkonko M.: Ubuntu in South Africa: a sociolinguistic perspective to a pan-African concept. Critical Arts, 1999, Vol. 13, No. 2, s. 24–41.

Lynskey 2014

Lynskey, Orla: Deconstructiong Data Protection: The Added-Value of a Right to Data Preotection in the EU Legal Order. International and Comparative Law Quarterly, Vol. 63, 2014, s. 569–597.

Lynskey 2015

Lynskey, Orla: The Foundations of EU Data Protection Law. Oxford 2015.

Makulilo 2012

Makulilo, Alex Boniface: Privacy and data protection in Africa: a state of the art. International Data Privacy Law, 2012, Vol. 2, No. 3, s. 163–178.

Manners 2002

Manners, Ian: Normative Power Europe: a Contradiction in Terms? Journal of Common Market Studies, 2002, Vol. 40, No. 2, s. 235–258.

Mayer-Schönberger 2009

Mayer-Schönberger, Viktor: delete. The Virtue of Forgetting in the Digital Age. New Jersey 2009.

Olinger et al. 2007

Olinger, Hanno N. – Britz, Johannes J. – Olivier, Martin S.: Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy

bill in South Africa. The International Information & Library Review, 2007, Vol. 39, s. 31–43.

Parker 1974

Parker, Richard B.: A Definition of Privacy. Rutgers Law Review, 1974, Vol. 27, No. 2, s. 275–296.

Pekkanen 1997

Pekkanen, Raimo: Tuomiovalta ja tiedotusvälineet. Lakimies, 1997, No. 1, s. 17–24.

Rickless 2007

Rickless, Samuel C.: The Right to Privacy Unveiled. San Diego Law Review, 2007, Vol. 44, s. 773–800.

Rosas 2011

Rosas, Allan: Perus- ja ihmisoikeudet EU-oikeudessa. Teoksessa Perusoikeudet (toim. Pekka Hallberg). Helsinki 2011.

Rosen 2012

Rosen Jeffrey: The Right to Be Forgotten. Stanford Law Review Online, 13.2.2012. https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/

Rubel 2007

Rubel, Alan: Some Questions for the Barrier Theory. San Diego Law Review, 2007, Vol. 44, s. 801–808.

Salbu 2002

Salbu, Steven R.: The European Union Data Privacy Directive and International Relations. Vanderbilt Journal of Transnational Law, 2002, Vol. 35, Is. 2, s. 655–695.

Senz – Charlesworth 2001

Senz, Deborah – Charlesworth, Hilary: Building Blocks: Australia's Response to Foreign Extraterritorial Legislation. Melbourne International Law Review, 2001, Vol. 2, s. 69–121.

Solove 2009

Solove, Daniel J.: Understanding Privacy. Cambridge, Massachusetts 2009.

Stute 2015

Stute, David J.: Privacy Almighty? The CJEU's Judgement in Google Spain SL. v. AEDP. Michigan Journal of International Law, 2015, Vol. 36, s. 649–680.

Sunstein 2014

Sunstein, Cass R.: Why Nudge? The Politics of Libertarian Paternalism. New Haven & London 2014.

Svantesson 2014

Svantesson, Dan Jerker B.: The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and Its Practical Effect on US Business. Stanford Journal of International Law, 2014, Vol. 50, Is. 1, s. 53–102.

Taylor 2017

Taylor, Mistale: Google Spain Revisited: The Misunderstood Implementation of a Landmark Decision and How Public International Law Could Offer Guidance. Data Protection Law Review, 2017, Is. 2, s. 195–208.

Thaler – Sunstein 2003

Thaler, Richard H. – Sunstein, Cass R.: Libertarian Paternalism. The American Economic Review, 2003, Vol. 93, No. 2, s. 175-179.

Thomson 1975

Thomson, Judith Jarvis: The Right to Privacy. Philosophy & Public Affairs, 1975, Vol. 4, No. 4, s. 295–314.

Twining 1997

Twining, William: Law in Context. Enlarging a Discipline. Oxford 1997.

Twining 2009

Twining, William: General Jurisprudence. Understanding Law from a Global Perspective. Cambridge 2009.

Ustaran 2018

Ustaran, Eduardo: International Data Transfers, teoksessa European Data Protection. Law and Practice (ed. Eduardo Ustaran). Portsmouth 2018.

van Bavel – Rodríguez-Priego 2016

van Bavel, René – Rodríguez-Priego, Nuria: Nudging Online Security Behaviour with Warning Messages. Results from an online experiment. The Joint Research Centre (JRC) Technical Reports. 2016, EUR 28197 EN.

Volio 1981

Volio, Fernando: Legal Personality, Privacy, and the Family. s. 185–208 teoksessa The International Bill of Rights. The Covenant on Civil and Political Rights. (toim. Henkin, Louis). New York 1981.

Warren – Brandeis 1890

Warren, Samuel D. – Brandeis, Louis D.: The Right to Privacy. Harvard Law Review, 1890–1891, Vol 5, No. 4, s. 193–220.

Whitman 2004

Whitman, James Q.: The Two Western Cultures of Privacy: Dignity versus Liberty. Yale Law Journal, 2004, Vol. 113, s. 1151–1221.

Zielonka 2008

Zielonka, Jan: Europe as a global actor: empire by example? International Affairs, 2008, Vol 84, No. 3, s. 471–484.

Young 2015

Young, Alasdair R.: The European Union as a global regulator? Context and comparison. Journal of European Public Policy, 2015, Vol. 22, Is. 9, s. 1233–1252.

Oikeustapaukset

EIT

Klass ja muut v. Saksa, no. 5029/71, 6.9.1978.

Malone v. UK, no. 8691/79, 2.8.1984.

Niemietz v. Saksa, no. 13710/88, 16.12.1992.

Campmany y Diez de Revenga ja Lopez-Galiacho Perona v. Espanja, no. 54224/00, 12.12.2000.

Bou Gibert ja el Hogar y la Moda S.A. v. Espanja, no. 14929/02, 13.5.2003.

von Hannover v. Saksa, no. 59320/00, 24.6.2004.

Weber ja Saravia vs. Saksa, no. 54934/00, 29.6.2006

Axel Springer AG v. Saksa, no. 39954/08, 7.2.2012.

England and Wales High Court (the Queen's Bench Division)

EWHC 799, NT 1 & NT 2 v. Google LLC, 13.4.2018.

EUT

C-26/62 Van Gend en Loos

C-6/64 Costa v. ENEL

C-106/77 Simmenthal

C-101/01 Bodil Lindqvist

C-73/07 Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy ja Satamedia Oy

C-92/09 Volker ja Markus Schecke ja Eifert v. Land Hessen

C-366/10 Air Transport Association of America, American Airlines Inc., Continental Airlines Inc. ja United Airlines Inc. v. Secretary of State for Energy and Climate Change

C-131/12 Google Inc. ja Google Spain SL v. AEPD ja Mario Costeja González

C-362/14 Maximillian Schrems v. Data Protection Commissioner

Supreme Court of Canada

Google Inc. v. Equustek Solutions Inc., 2017 SCC 34, [2017] 1 S.C.R. 824, 28.6.2017.

U.S. District Court, Northern District of California (San Jose Division)

Google LLC v. Equustek Solutions Inc., Case No. 5:17-cv-04207-EJD, 2.11.2017.

Internetlähteet

https://e-estonia.com/free-movement-of-data-as-the-5th-fundamental-freedom-of-the-european-union/ (vierailtu 29.8.2018)

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en (vierailtu 23.8.2018)

http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm (vierailtu 24.9.2018)

https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain (vierailtu 18.5.2018)

https://hbr.org/2018/05/how-gdpr-will-transform-digital-marketing (vierailtu 18.5.2018)

http://indicators.ohchr.org/ (vierailtu 31.3.2018)

https://support.google.com/transparencyreport/answer/7347822 (vierailtu 11.6.2018)

https://transparencyreport.google.com/eu-privacy/overview (vierailtu 21.9.2018)

https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_en (vierailtu 11.4.2018)

http://www.bbc.com/news/world-asia-china-34592186 (vierailtu 7.8.2018)

https://www.bing.com/webmaster/tools/eu-privacy-request (vierailtu 5.7.2018)

https://www.cia.gov/library/publications/the-world-factbook/rankorder/2001rank.html#ch (vierailtu 4.10.2018)

https://www.eipa.eu/dataprotection/ (vierailtu 29.11.2018)

https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=0-636663760383976871-1219462126&rd=1 (vierailtu 5.7.2018)

https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights (vierailtu 6.9.2018)

https://www.privacyconference2018.org/ (vierailtu 29.11.2018)

https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/ (vierailtu 7.8.2018)

https://www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed (vierailtu 4.7.2018)

https://www.theguardian.com/technology/2017/jul/27/facebook-free-basics-developing-markets (vierailtu 11.4.2018)

https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (vierailtu 7.8.2018)

https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (vierailtu 10.9.2018)

https://www.wired.com/2008/04/eu-tells-search/ (vierailtu 8.8.2018)

https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?noredirect=on&utm_term=.0a970386ca93 (vierailtu 10.9.2018)

http://www.yk.fi/node/227 (vierailtu 12.4.2018)

https://yle.fi/uutiset/3-10135093 (vierailtu 7.8.2018)